Jumio's Motion to Strike FaceTec's Infringement Contentions

EXHIBIT 7

EXHIBIT E

F. Christopher Austin, Esq. (NV Bar No. 6559)
caustin@weidemiller.com
WEIDE & MILLER, LTD.
10655 Park Run Drive, Suite 100
Las Vegas, NV 89144
Tel: (702) 382-4804
Fax: (702) 382-4805

Nathaniel L. Dilger (CA Bar No. 196203)
ndilger@onellp.com
Peter R. Afrasiabi (CA Bar No. 193336)
pafrasiabi@onellp.com
William J. O'Brien (CA Bar No. 99526)
wobrien@onellp.com
ONE LLP
23 Corporate Plaza
Suite 150-105
Newport Beach, CA 92660
Tel: (949) 502-2870
Fax: (949) 258-5081

Attorneys for Plaintiff and Counter-Defendant, FaceTec, Inc.

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

FACETEC, INC., a Delaware corporation, Plaintiff, v. iPROOV LTD, a United Kingdom limited liability company, Defendant.	Case No. 2:21-cv-02252-ART-BNW **PLAINTIFF FACETEC. INC.'S AMENDED DISCLOSURE OF ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS**
iPROOV LTD, a United Kingdom limited liability company, Counter-Claimant, v. FACETEC, INC., a Delaware corporation, Counter-Defendant.	

Under Fed. R. Civ. P. 26 and Patent Local Rules 1-6 et. seq. and by agreed Order of the Court, Plaintiff and Counter-Defendant, FaceTec, Inc., hereby submits the following Amended Disclosure of Asserted Claims and Infringement Contentions. Pursuant to Local Patent Rule 1-12, FaceTec reserves the right to amend or supplement this disclosure based upon further analysis and discovery, including in response to the discovery responses and materials produced by the Defendant in this matter, and/or in response to the Court's claim construction order or other rulings in this matter.

A. FaceTec LPR 1-6(a) and 1-6(b) Disclosures.

FaceTec contends that Defendant and Counterclaimant, iProov Ltd., has infringed and is infringing at least claims 10, 13, 14, 15, 16, and 19 of the '471 patent and claims 1, 4-9, and 19-20 of the '606 patent.

Based on the public information currently available to it, FaceTec identifies the iProov instrumentalities infringing each of the foregoing claims as all iProov products and services (collectively, "Accused Instrumentalities") that (1) prompt a user to position their face at more than one distance from a user's device camera, and (2) collect face image data at at least two distances from the user's face and the device's camera.

FaceTec contends that the Accused Instrumentalities include at least all products that contain, or that iProov identifies as containing, "Liveness Assurance™ technology," including, without limitation, iProov's "Basic Face Verifier." *See, e.g.*, www.iproov.com/iproov-system/iproov-products-for-biometric-authentication/basic-face-verifier ("iProov Basic Face Verifier uses Liveness Assurance™ technology to confirm that an individual is the right person and provide some assurance that they are a real person.").

FaceTec provides information concerning the infringement of the foregoing patent claims by the Accused Instrumentalities in the charts below and attached Exhibits A and B, based on the information presently available to it. Determining whether there has been infringement of any of the remaining claims or infringement by other Accused Instrumentalities requires discovery regarding certain non-public aspects of that

technology. For this reason and pursuant to Local Patent Rule 1-12, FaceTec reserves the right to amend or supplement this disclosure based upon further analysis and discovery, including in response to the discovery responses and materials produced by the Defendant in this matter, and/or in response to the Court's claim construction order or other rulings in this matter.

1. U.S. Pat. No. 10,776,471

Claim	Claim Alleged to be Infringed by the Accused Instrumentalities?	Asserted Statutory Basis
10	Yes	35 U.S.C. §§ 271(a), (b), (c)
11	FaceTec cannot determine whether the Accused Instrumentalities infringe this claim until FaceTec obtains discovery regarding certain non-public aspects of iProov's verification technology.	
12	*See supra*, claim 11.	
13	Yes	35 U.S.C. §§ 271(a), (b), (c)
14	Yes	35 U.S.C. §§ 271(a), (b), (c)
15	Yes	35 U.S.C. §§ 271(a), (b), (c)
16	Yes	35 U.S.C. §§ 271(a), (b), (c)
17	*See supra*, claim 11.	
18	*See supra*, claim 11.	
19	Yes	35 U.S.C. §§ 271(a), (b), (c)
20	*See supra*, claim 11.	

/ / /

/ / /

2. U.S. Pat. No. 11,157,606 B2

Claim	Claim Alleged to be Infringed by the Accused Instrumentalities?	Asserted Statutory Basis
1	Yes	35 U.S.C. §§ 271(a), (b), (c)
2	FaceTec cannot determine whether the Accused Instrumentalities infringe this claim until FaceTec obtains discovery regarding certain non-public aspects of iProov's verification technology.	
3	*See supra*, claim 2.	
4	Yes	35 U.S.C. §§ 271(a), (b), (c)
5	Yes	35 U.S.C. §§ 271(a), (b), (c)
6	Yes	35 U.S.C. §§ 271(a), (b), (c)
7	Yes	35 U.S.C. §§ 271(a), (b), (c)
8	Yes	35 U.S.C. §§ 271(a), (b), (c)
9	Yes	35 U.S.C. §§ 271(a), (b), (c)
19	Yes	35 U.S.C. §§ 271(a), (b), (c)
20	Yes	35 U.S.C. §§ 271(a), (b), (c)

B. FaceTec LPR 1-6(c) Disclosures.

1. U.S. Pat. No. 10,776,471

FaceTec has provided a chart (**Exhibit A**) identifying specifically where each limitation of each asserted claim of the '471 patent is found within the Accused Instrumentalities.

2. U.S. Pat. No. 11,157,606 B2

FaceTec has provided a chart (**Exhibit B**) identifying specifically where each limitation of each asserted claim of the '606 patent is found within the Accused Instrumentalities.

C. FaceTec LPR 1-6(d) Disclosures.

For each claim above that is alleged to have been indirectly infringed, FaceTec provides herein and/or in the attached charts (1) an identification of the claims alleged to have been indirectly infringed, (2) an identification of the direct infringement, (3) a description of the alleged acts of indirect infringer that contribute to or are inducing that direct infringement, and (4) where the alleged direct infringement is based on joint acts of multiple parties, the identity and role of each party alleged to be involved in the acts of direct infringement.

1. FaceTec's identification of the asserted claims alleged to have been indirectly infringed.

To the extent any asserted claims are not directly infringed as set forth in FaceTec's 1-6(c) Disclosures herein, FaceTec alternatively asserts that Defendant has contributorily infringed and/or induced the infringement of at least claims 10, 13, 14, 15, 16, and 19 of the '471 patent and claims 1, 4-9, and 19-20 of the '606 patent as set forth in Sections A(1) and A(2), *supra*, and in the attached charts.

2. FaceTec's identification of the direct infringement.

FaceTec has identified in the attached charts the acts constituting direct infringement of at least claims 10, 13, 14, 15, 16, and 19 of the '471 patent (**Exhibit A**) and claims 1, 4-9, and 19-20 of the '606 patent (**Exhibit B**).

3. FaceTec's description of the alleged acts that contribute to or are inducing that direct infringement.

FaceTec contends that – to the extent that Defendants do not directly infringe any of the asserted claims as set forth herein and in the attached charts – Defendant indirectly infringes those claims. Defendant's acts of indirect infringement include inducement of infringement and contributory infringement under 35 U.S.C. §§ 271(b) and (c) as set forth in Sections A(1) and A(2), *supra*, and in the attached charts.

Defendant contributorily infringes the asserted patents by using, offering to sell, and selling within the United States and/or importing into the United States the Accused

Instrumentalities, including components of patented machines, manufactures, combinations, materials and/or apparatus for use in practicing the patented systems, processes or methods, which constitute a material part of the inventions, knowing the same to be especially made or especially adapted for use in an infringement of the asserted patents, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

By way of example, such indirect infringement includes offering customers and users access to the Accused Instrumentalities to be used in accordance with the claimed methods and systems, including certain user-supplied components, such as user-supplied computers, tablets, and smartphones.

Defendant has induced infringement of the asserted products by virtue of the activities described herein and in the attached charts, as well as by aiding, assisting, and abetting the practice of the patented inventions as set forth herein and in the attached charts. Such activities include Defendant's provision of web-based, phone-based, email-based and/or literature-based promotion, support and assistance with respect to utilizing the Accused Instrumentalities (*e.g.*, manuals, product guides, user forums, troubleshooting tips, and other forms of support and assistance for utilizing the Accused Instrumentalities). Such activities further include instructing Defendant's customers to utilize Accused Instrumentalities in an infringing manner and configuring the Accused Instrumentalities such that a user will be unable to obtain verification unless the Accused Instrumentalities are used in an infringing manner.

As one example, during an authentication session, iProov will specifically instruct users to utilize iProov's Accused Instrumentalities in a manner that infringes the Asserted Claims. Indeed, unless the users follow the specific instructions provided by Defendant to utilize the Accused Instrumentalities in an infringing manner, the Accused Instrumentality will not verify the physical presence of the user.

Defendant's additional activities include creation, provision, distribution, and promotion of instructions, user guides and other product-related documentation,

technical support, video tutorials, training and certification, user forums, professional consultation, warranty support, indemnification, technical notes, release notes, articles, etc., for utilizing the Accused Instrumentalities. These include forums hosted by Defendant dedicated to integrating the Accused Instrumentalities into other software platforms or applications for eventual use in those software platforms or applications in an infringing manner. *See, e.g.*, www.iproov.com/iproov-system/technology/iproov-integrations; https://github.com/iProov.

Pursuant to Local Patent Rule 1-12, FaceTec reserves the right to amend or supplement this disclosure based upon further analysis and discovery, including in response to the discovery responses and materials produced by the Defendant in this matter, and/or in response to the Court's claim construction order or other rulings in this matter.

4. Where the alleged direct infringement is based on joint acts of multiple parties, FaceTec provides the following identity and role of each party alleged to be involved in the acts of direct infringement.

FaceTec has identified in the attached exhibits the parties involved in the acts of direct infringement and each party's role in those acts for at least claims 10, 13, 14, 15, 16, and 19 of the '471 patent (Exhibit A) and claims 1, 4-9, and 19-20 of the '606 patent (Exhibit B).

Typically, Defendant iProov will provide each of its customers ("Customer") access to the Accused Instrumentalities. The Customer will utilize the Accused Instrumentalities to confirm that individuals ("Users") who might be seeking access to systems and resources of the Customer are properly verified. A typical iProov/Customer/User arrangement is shown in the data flow diagram below:

/ / /

/ / /

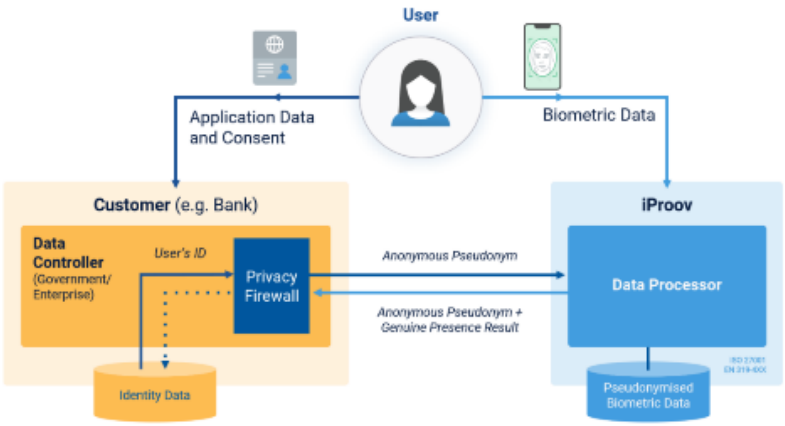


Fig. 2: The Data Controller is iProov's Customer, iProov is the Data Processor

In the example depicted above, the Customer is a bank, which has contracted with Defendant iProov to provide access to the Accused Instrumentalities. The bank incorporates iProov's Accused Instrumentalities to confirm that individuals seeking access to, for example, their bank account are first properly verified.

In the example above, the User will typically utilize a smartphone, tablet, computer, or other similar device to request online access to their bank account. The User's request would then be routed in some fashion (typically via an online portal provided by the bank) to iProov, which implements the Accused Instrumentalities to verify the identity of the User who is seeking access. As explained above and in the accompanying exhibits, the Accused Instrumentalities instructs the User – both via onscreen instructions and via onscreen "ovals" – to vary the distance between the User the device camera so that the device camera can captures at least two images at varying distances. The Accused Instrumentalities then utilizes these images to verify the User. The bank will then be notified by the Accused Instrumentalities that the User has been verified and the User is then permitted access to his/her account at the bank.

D. FaceTec LPR 1-6(e) Disclosures.

FaceTec alleges that – based on its current understanding of the proper construction of the Asserted Claims and at this early stage in the litigation without the benefit of complete discovery from Defendant regarding the Accused Instrumentalities –

each limitation of each such claim is alleged to be literally present in the Accused Instrumentalities. FaceTec reserves the right to assert infringement under the doctrine of equivalents upon receiving the Court's claim construction or after further discovery.

E. FaceTec LPR 1-6(f) Disclosures.

FaceTec alleges that each asserted claim of the '471 patent is entitled to a priority date of at least Aug. 28, 2015. FaceTec alleges that each asserted claim of the '606 patent is entitled to a priority date of at least Aug. 28, 2015.

F. LPR 1-6(g) Disclosures.

FaceTec contends that least claims 10, 13, 14, 15, 16, and 19 of the '471 patent and claims 1, 4-9, and 19-20 of the '606 patent are practiced by all of versions of FaceTec's 3D Liveness Detection software and/or the use of the same.

G. FaceTec LPR 1-6(h) Disclosures.

FaceTec alleges that Defendant's infringement of the '471 and '606 patents has been willful. For example, as alleged in FaceTec's First Amended Complaint [D.E. 18], Defendant wrongfully participated in FaceTec's Bounty Program for the primary purpose of reverse engineering various aspects of FaceTec's patented technology. iProov then added information improperly gleaned from this reverse engineering to create the infringing "Liveness Assurance" technology.

In addition, Defendant has continued to utilize the infringing "Liveness Assurance" technology despite having actual knowledge of the '471 and '606 patents and actual knowledge that the "Liveness Assurance" technology infringes those patents. For example, FaceTec contacted iProov in writing on or about September 9, 2021, demanding that iProov immediately cease and desist its improper use of any and all technology learned by iProov during its exhaustive reverse engineering as well as specifically identifying the '471 patent and providing a chart explaining how iProov's "Liveness Assurance" infringed at least one claim of that patent. In that letter, FaceTec demanded that iProov cease and desidt from infringement. While iProov responded to this letter shortly thereafter, it refused FaceTec's demand to cease and desist and refused

to address the unauthorized use of information it learned regarding FaceTec's Liveness detection software.

On February 16, 2022, FaceTec again contacted iProov, this time to identify the '606 patent and to explain how iProov's "Liveness Assurance" technology infringed that patent. iProov, however, did not respond to this communication.

Despite having been notified that the "Liveness Assurance" technology infringed both the '471 and '606 patents, Defendant has continued to offer and provide this technology to customers. This has continued not only after FaceTec's letters of September 9, 2021, and February 16, 2022, but even after FaceTec's filing of its original Complaint and then its First Amended Complaint in this action.

Pursuant to Local Patent Rule 1-12, FaceTec reserves the right to amend or supplement this disclosure based upon further analysis and discovery, including in response to the discovery responses and materials produced by the Defendant in this matter, and/or in response to the Court's claim construction order or other rulings in this matter.

Dated: July 26, 2023

ONE LLP

/s/ Nathaniel L. Dilger

Nathaniel L. Dilger (*pro hac vice*)
Peter R. Afrasiabi (*pro hac vice*)
William J. O'Brien (*pro hac vice*)
23 Corporate Plaza
Suite 150-105
Newport Beach, CA 92660
Email: ndilger@onellp.com
pafrasiabi@onellp.com
wobrien@onellp.com

WEIDE & MILLER, LTD.
F. Christopher Austin (SBN 6559)
10655 Park Run Drive, Suite 100
Las Vegas, NV 89144
Tel: (702) 382-4804
Fax: (702) 382-4805
Email: caustin@weidemiller.com

Attorneys for Plaintiff and Counter-Defendant FaceTec, Inc.

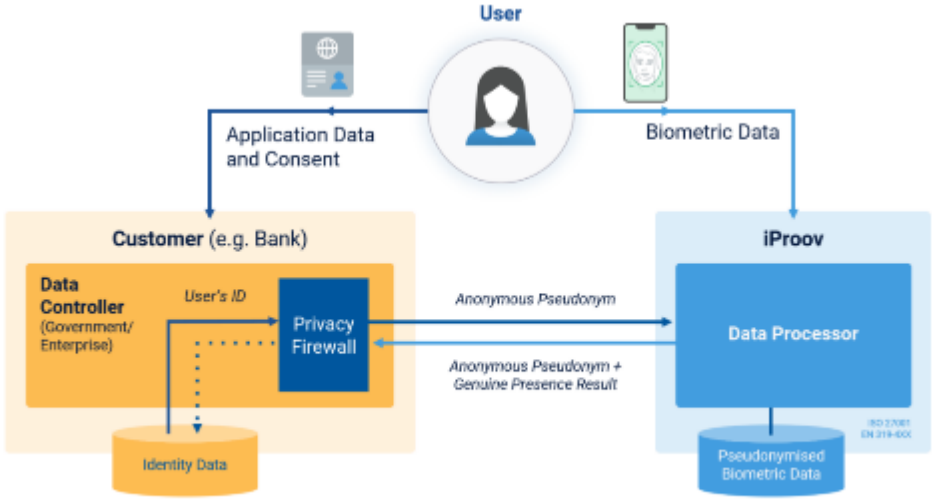
EXHIBIT A

Exhibit A: FaceTec U.S. Patent No. 10,776,471

'471 Patent Claim Language	Accused Instrumentality
10. A method for authenticating three-dimensionality of a user via a user's camera equipped computing device, the method, during an authentication session comprising:	The Accused Instrumentality uses images of a user's face captured using a camera equipped computing device (e.g., a camera-equipped smartphone, computer, or tablet) to attempt to verify one or more user characteristics and thereby verify the physical presence of the user. *See* www.iproov.com/iproov-system/technology/liveness-assurance. One aspect that the Accused Instrumentality verifies is three-dimensionality of the user's face as compared to, for example, a two-dimensional photograph. www.iproov.com/videos/liveness-assurance (the Accused Instrumentality confirms that a user is "a real person … [and] not a photograph.")

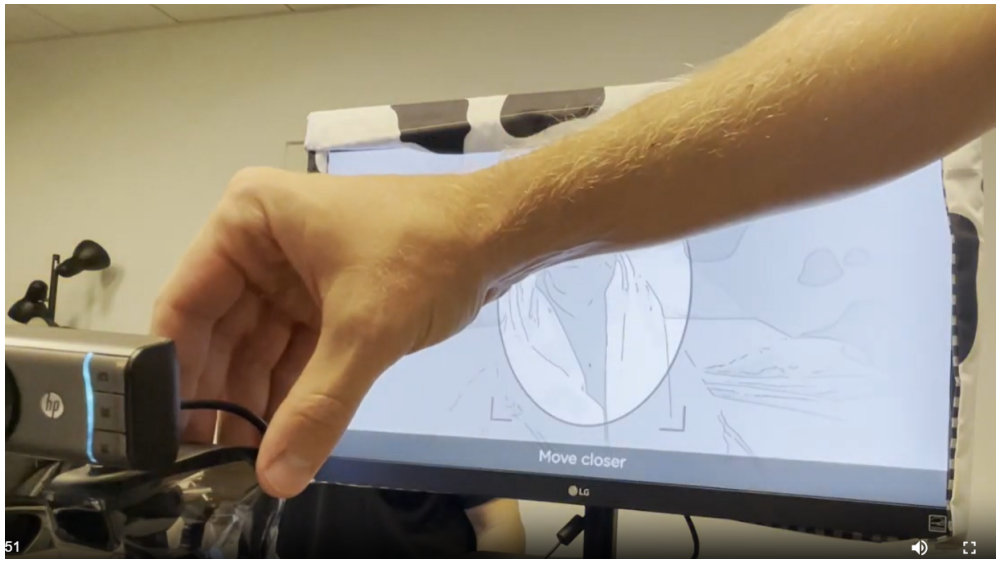
capturing at least one first image of the user taken with the camera of the computing device at a first location which is a first distance from the user;	During face data capture the Accused Instrumentality prompts the user to position their face at least two distances from the camera, during which the Accused Instrumentality collects at least two images of the user's face. These at least two images are collected at different distances between the user's face and the device camera. The following images are taken from actual Liveness Assurance authentication sessions. Using a combination of on screen prompts and manipulation of the video shown in the background, the Accused Instrumentality induces the user to change the distance between the device and the user so that images of the user's face are captured at two distances. For example, the Accused Instrumentality manipulates the user to change the distance between the device and the user so that the user's face is framed within the "oval" provided on the device's screen. 1. As shown below, the system prompts the user to "put your face in the frame."  2. After the user frames their face in the oval, the Accused Instrumentality captures at least one image of the user, which image is taken at a first distance.

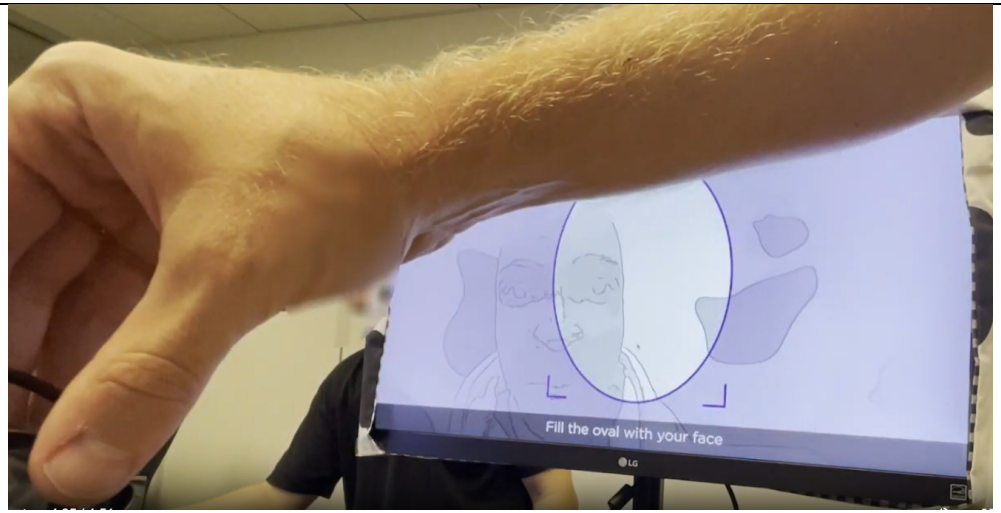
processing the at least one first image or a portion to create first data;	During the image capture process described herein, the Accused Instrumentality typically captures approximately 10 image frames of the user. The Accused Instrumentality packages these images into a "WebM payload," which the user's device then sends to iProov's server for data processing. Using the publicly available Chrome Dev Tools Network Tab (developer.chrome.com/docs/devtools/network/), one can examine the contents of this WebM payload, which the Accused Instrumentality sends in unencrypted format. Below are several image frames taken from the WebM payload filed created during a Liveness Assurance authentication session. As can be seen, image frames are collected at different distances between the user and the camera:  *See also* docs.iproov.com/docs/Content/ImplementationGuide/api/api-optional-features.htm ("You can optionally request the image of the user that is captured during an enroll validate or claim validate process. The following frame will be provided in the API response: LA: last frame [and] GPA: 4th frame.")

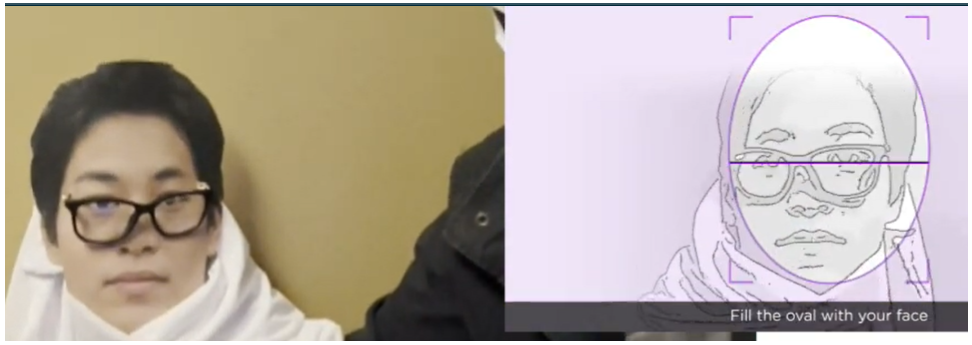
	As shown in iProov's data flow chart below, the iProov server receives from the user's device this WebM payload, which includes "biometric data" including "first data" comprised of or based on the at least one first image of the user's face captured by the Accused Instrumentality and at least one other image of the user's face captured at a different distance.  **Fig. 2: The Data Controller is iProov's Customer, iProov is the Data Processor** iProov explains how the Accused Instrumentality uses the user's captured biometric data for enrollment and face matching / recognition / verification. ***Enrollment:*** The process of collecting a user's biometric data for the first time. The data is encrypted and sent to a server, binding a verified identity with a biometric to a legitimate account or service. ***Face matching:*** Comparing one face to another to confirm it is the right person. During enrollment a biometric face capture is compared to a photo on an identity document. During authentication the captured biometric data is compared to a previously enrolled biometric template. ***Face recognition:*** Technology that matches face biometric data of a user, or users, against an image or database of legitimate information. Typically used as part of a user verification process.

Case 3:24-cv-02263-RFL NW Document 89-6 Filed 08/19/24 Page 17 of 78

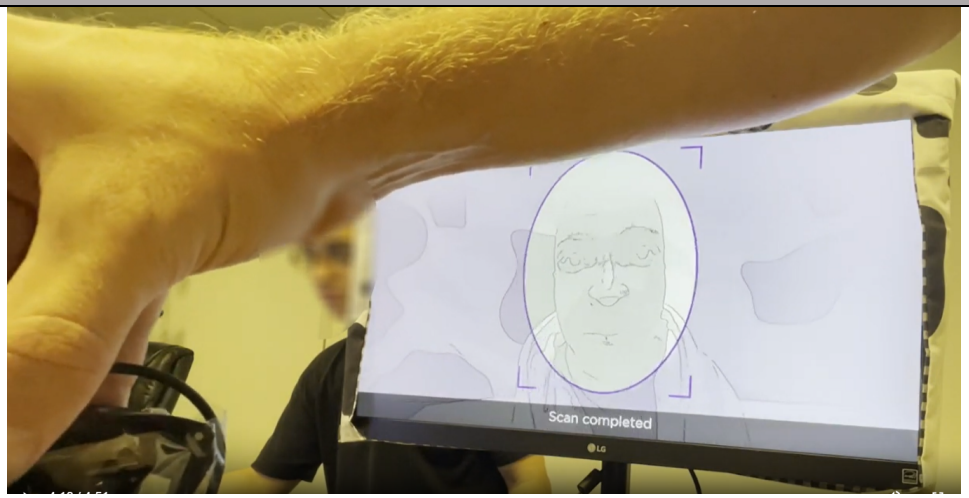
’471 Patent Claim Language	Accused Instrumentality
	Face verification: Matching the biometric data of the subject user to the biometric data of the expected user. *See* docs.iproov.com/docs/Content/Glossary/iproov-glossary.htm

moving the camera from the first location to a second location, the second location being a second distance from the user, or the user moving from the first location to the second location to change the distance between the user and the camera from the first distance to a second distance; [and] capturing at least one second image of the user taken with the camera of the computing device at the second distance from the user, the second distance being different than the first distance;	During face data capture the Accused Instrumentality prompts the user to position their face at least two distances from the camera, during which the Accused Instrumentality collects at least two images of the user's face. These at least two images are collected at different distances between the user's face and the device camera. 3. After capturing the at least one first image of the user's face (described above), the system changes the visible background resolution and instructs the user to "move closer" and to "fill the oval with your face." This can be seen in the images below: 

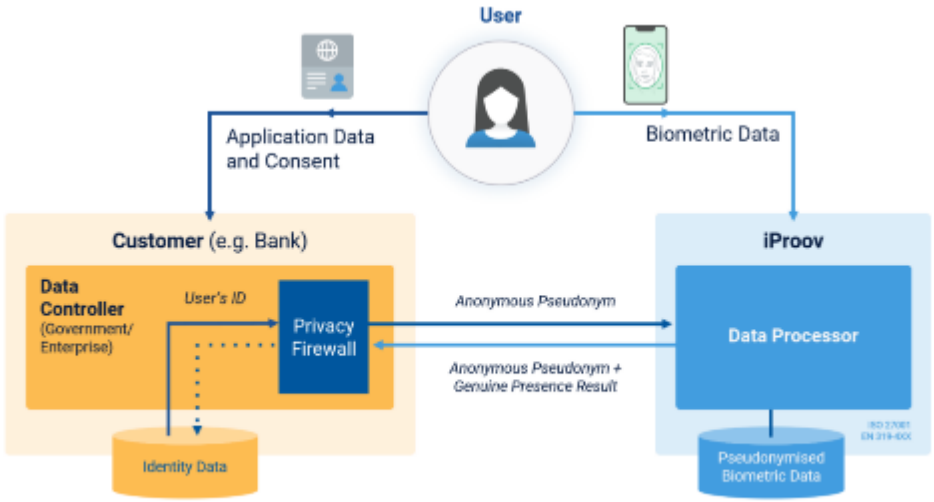




4. As the user changes the distance between their face and the camera as a result of the prompts so as to fill the oval with their face, the camera captures multiple additional images of the user, including at least one second image at a second distance different from the first distance.
5. After capturing the at least one first and second images of the user, the Accused Instrumentality then displays to the user “scan completed.” This can be seen in the image below.

’471 Patent Claim Language	Accused Instrumentality
	

processing the at least one second image or a portion thereof to create second data;	During the image capture process described herein, the Accused Instrumentality captures approximately 10 image frames of the user. The Accused Instrumentality packages these images into a "WebM payload," which the user's device then to iProov's server for data processing. Using the publicly available Chrome Dev Tools Network Tab (developer.chrome.com/docs/devtools/network/), one can examine the contents of this WebM payload, which the Accused Instrumentality sends in unencrypted format. Below are several image frames taken from the WebM payload filed created during a Liveness Assurance authentication session. As can be seen, image frames are collected at different distances between the user and the device camera:  *See also* docs.iproov.com/docs/Content/ImplementationGuide/api/api-optional-features.htm ("You can optionally request the image of the user that is captured during an enroll validate or claim validate process. The following frame will be provided in the API response: LA: last frame [and] GPA: 4th frame.")

	As shown in iProov's data flow chart below, the iProov server receives from the user's device this WebM payload, which includes "biometric data" containing the "first data" and including "second data" comprised of or based on the at least one second image of the user's face captured by the Accused Instrumentality.  **Fig. 2: The Data Controller is iProov's Customer, iProov is the Data Processor** iProov explains how the Accused Instrumentality uses the user's captured biometric data for enrollment and face matching / recognition / verification. ***Enrollment:*** The process of collecting a user's biometric data for the first time. The data is encrypted and sent to a server, binding a verified identity with a biometric to a legitimate account or service. ***Face matching:*** Comparing one face to another to confirm it is the right person. During enrollment a biometric face capture is compared to a photo on an identity document. During authentication the captured biometric data is compared to a previously enrolled biometric template. ***Face recognition:*** Technology that matches face biometric data of a user, or users, against an image or database of legitimate information. Typically used as part of a user verification process.

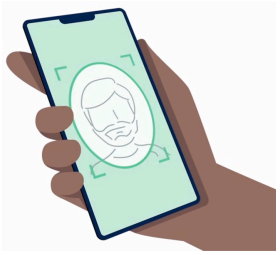
'471 Patent Claim Language	Accused Instrumentality
	Face verification: Matching the biometric data of the subject user to the biometric data of the expected user. *See* https://docs.iproov.com/docs/Content/Glossary/iproov-glossary.htm

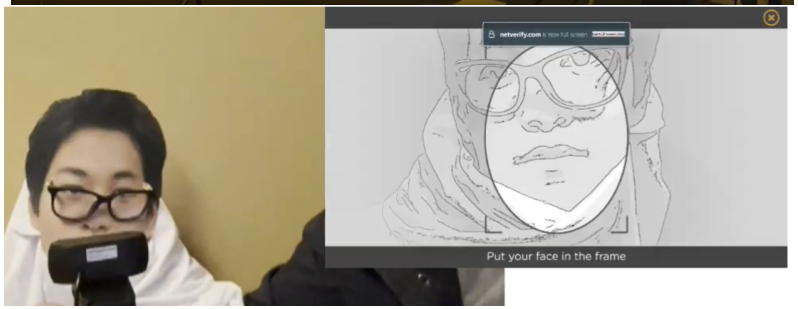
comparing the first data to the second data to determine whether expected distortion exist between the first data and the second data which indicated three-dimensionality of the user; and	The iProov Server receives biometric information regarding the user, including the first biometric data and the second biometric data discussed above. iProov has confirmed that the Accused Instrumentality operates using a neural network ("iProov Neural Network"): > "By default, the technology picks up certain cues on the face to detect that it is actually human. This uses technology that learns on an ongoing, continuous basis. So, the solution deploys deep convolutional neural network and computer vision technology, which uses machine learning algorithms. Thus, the idea is that more people can authenticate themselves. The person goes through the authentication process; the algorithm learns to understand the behavior of the human face based on how the person's features change over time or how they respond while looking at the screen. This is how iProov uses deep learning technology in our biometric product." https://itsecuritywire.com/interviews/remote-identification-process-simplified-and-safeguarded-by-the-biometr; *see also* https://docs.iproov.com/docs/Content/Overview/biometric-assurance.htm ("Liveness Assurance is a patented 3D passive face biometric verification technology that combines camera imagery and contextual data from the authentication process. Powerful deep learning AI methods assure accurate face matching and determine liveness."); **Liveness Assurance** Liveness Assurance is a patented 3D passive face biometric verification technology that combines camera imagery and contextual data from the authentication process. Powerful deep learning AI methods assure accurate face matching and determine liveness. LA has these benefits: • Delivers a simple, passive, and low ceremony user experience. • Provides assurance it's a **real** person and the **right** person. • Defends against known digital or physical presentation attacks and camera bypass digital attacks.

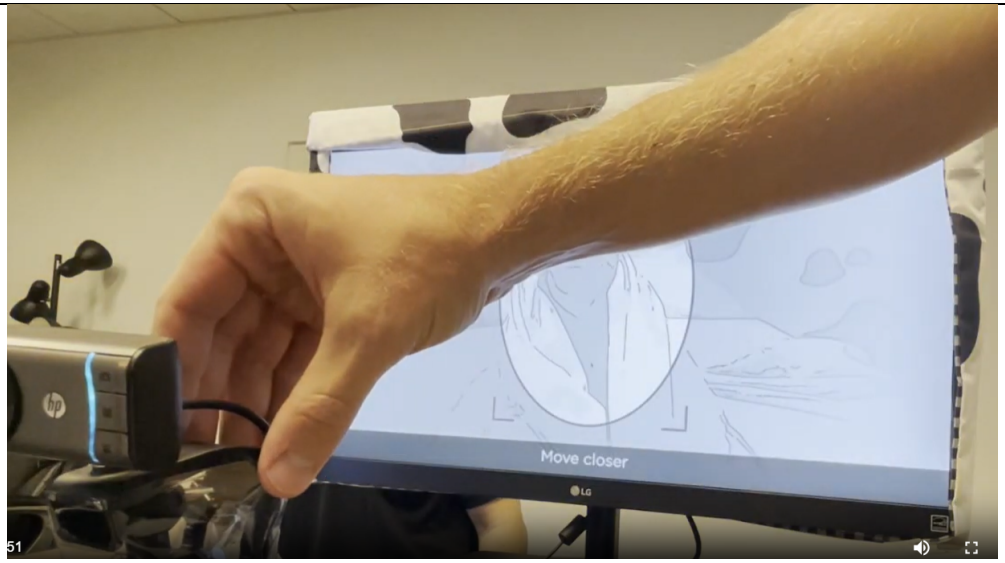
’471 Patent Claim Language	Accused Instrumentality
	The iProov Neural Network necessarily analyzes all data provided to it to verify to a high level of confidence that the user is three-dimensional. www.iproov.com/videos/liveness-assurance (the Accused Instrumentality confirms that a user is “a real person … [and] not a photograph.”). The iProov Neural Network verifies this based at least in part on analyzing the first data and the second data. The iProov Neural Network internally compares the first data and the second data to identify similarities and differences therebetween. This comparison includes (1) whether the first biometric data has differences from the second biometric data, and (2) whether the face image represented in the first biometric data and the face image represented in the second biometric data displays the expected distortion between the images that should be observed between an image of a three-dimensional user’s face taken at the first distance and an image of a user’s three-dimensional face taken at the second distance. *See, e.g.*, IP-00003260; *see also* IP-00003256-61. The Accused Instrumentality requires no change (facial or otherwise) other than a change in distance (and potentially face realignment within the oval) between the user and the device.

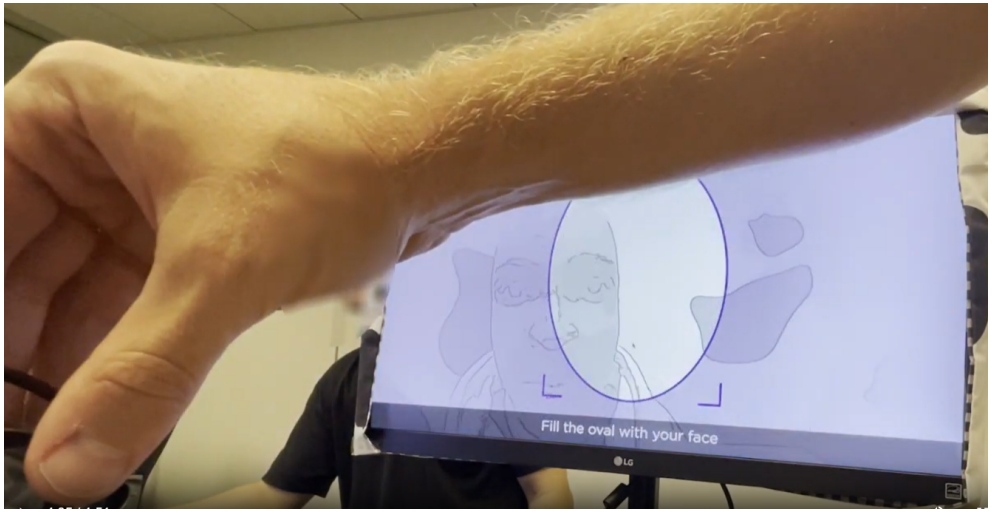
’471 Patent Claim Language	Accused Instrumentality
authenticating the user when the differences between the first data and the second data have expected distortion resulting from movement of the camera from the first location to the second location or movement of the user from the first location to the second location which causes the change in distance between the user and the camera.	FaceTec has tested the Accused Instrumentality to confirm that, if expected distortion between the first biometric data and the second biometric data does not match expected distortion between an image of a user’s three-dimensional face taken at the first distance and an image of a user’s three-dimensional face taken at the second distance, the Accused Instrumentality will normally not confirm that the user is physically present. For example, FaceTec tested the Accused Instrumentality and confirmed that it will not normally confirm the user is physically present when a two-dimensional photo of the user is used. *See*, e.g., www.iproov.com/videos/liveness-assurance (the Accused Instrumentality confirms that a user is “a real person … [and] not a photograph.”). Conversely, FaceTec has tested the Accused Instrumentality and confirmed that, if expected distortion between the first data and the second data matches expected distortion between an image of a user’s three-dimensional face taken at the first distance and an image of a user’s three-dimensional face taken at the second distance, the Accused Instrumentality will normally confirm that the user’s face is three-dimensional and that the user is likely to be physically present. For example, FaceTec tested the Accused Instrumentality and confirmed that Accused Instrumentality will normally confirm the user is physically present when a three-dimensional user conducts the verification steps outlined above. As shown in the images reproduced above, FaceTec tested the Accused Instrumentality using both a three dimensional “doll” head as well as a two-dimensional photo that had been modified with both a shawl and a pair of eyeglasses, both of which the Accused Instrumentality verified.

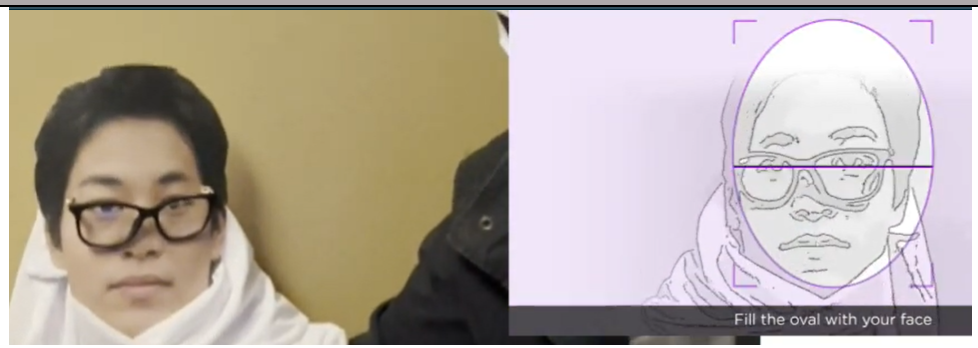
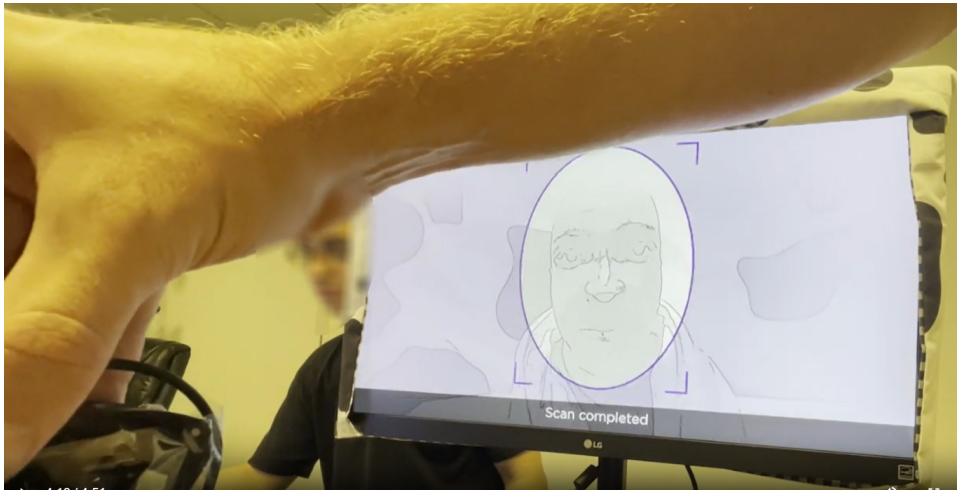
’471 Patent Claim Language	Accused Instrumentality
11. The method according to claim 10, further comprising: interpolating the first data and the second data to obtain estimated intermediate data; capturing at least one third image of the user taken with the camera of the computing device at a third distance from the user, the third distance being between the first distance and the second distances; processing the at least one third image or a portion thereof to obtain third data; and comparing the estimated intermediate data with the third data to determine whether the third data matches the estimated intermediate data.	FaceTec cannot determine whether the Accused Instrumentality infringes this claim until FaceTec obtains discovery regarding certain non-public aspects of iProov’s verification technology.
12. The method according to claim 10, further comprising verifying the presence of the user's ears in the at least one first image, and verifying the absence or reduced visibility of the user's ears in the at least one second image, wherein the first distance is larger than the second distance.	FaceTec cannot determine whether the Accused Instrumentality infringes this claim until FaceTec obtains discovery regarding certain non-public aspects of iProov’s verification technology.

13. The method according to claim 10, wherein the computing device is configured to display one or more prompts on a screen of the computing device to guide the user to capture the at least one first image at the first distance and the at least on second image at the second distance.	During face data capture the Accused Instrumentality prompts the user to position their face at least two distances from the camera, during which the Accused Instrumentality collects at least two images of the user's face. These at least two images are collected at different distances between the user's face and the device camera. Using on-screen prompts, the Accused Instrumentality directs the user to adjust the distance between the camera and the user so that the user's face is framed within an "oval" provided on the device's screen.  *See* www.iproov.com/what-we-do/use-cases/authentication The following images are taken from actual Liveness Assurance authentication sessions. Using a combination of on screen prompts and manipulation of the video shown in the background, the Accused Instrumentality induces the user to change the distance between the device and the user so that images of the user's face are captured at two distances. For example, the Accused Instrumentality manipulates the user to change the distance between the device and the user so that the user's face is framed within the "oval" provided on the device's screen.

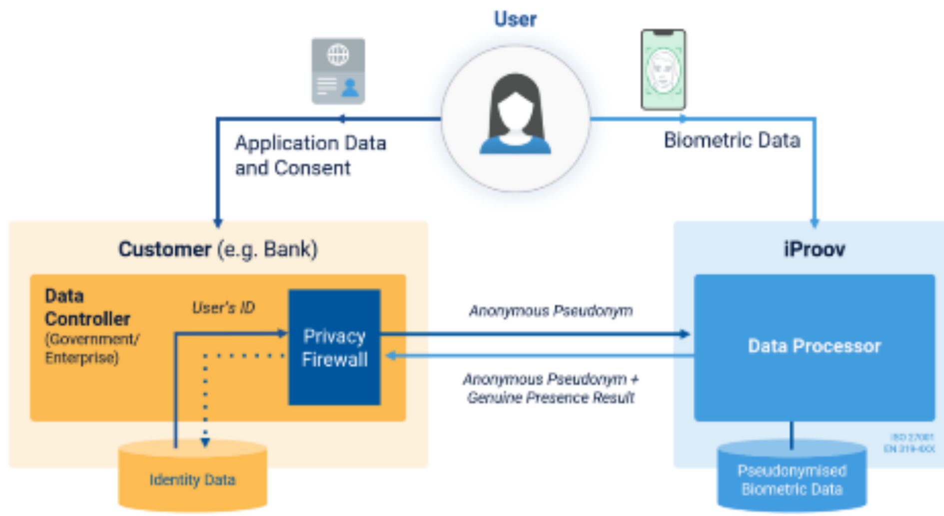
	1. As shown below, the system prompts the user to "put your face in the frame."   2. After the user frames their face in the oval, the Accused Instrumentality captures at least one image of the user, which image is taken at a first distance. 3. After capturing the at least one first image of the user's face (described above), the system changes the background resolution that is displayed and prompts the user to "move closer" and to "fill the oval with your face." This can be seen in the images below:


Move closer

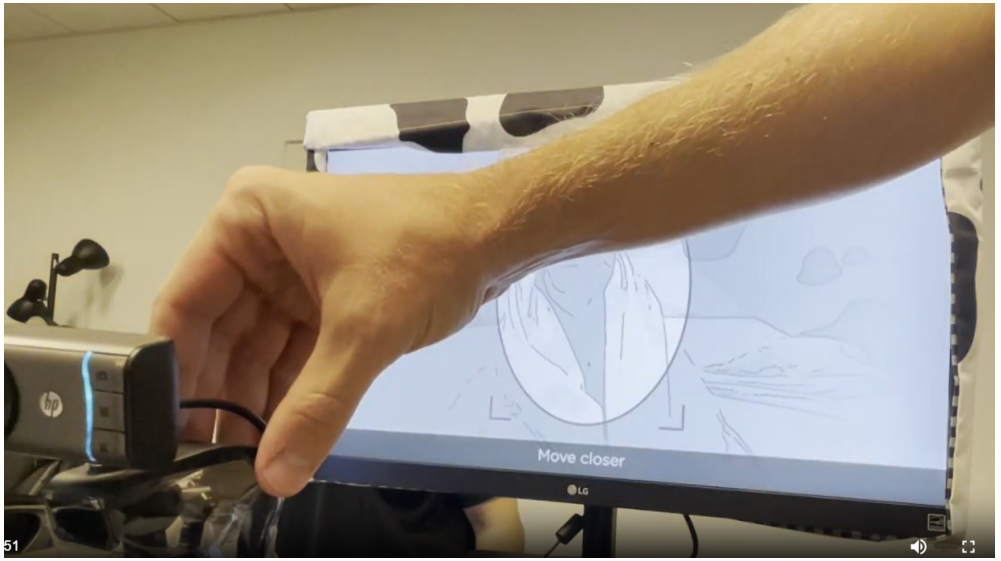

Fill the oval with your face

’471 Patent Claim Language	Accused Instrumentality
	 4. As the user changes the distance between their face and the camera so as to fill the oval with their face, the camera captures multiple additional images of the user, including at least one second image that is captured at a second distance different from the first distance. 5. After capturing the at least one first and second images of the user, the Accused Instrumentality then displays to the user “scan completed.” This can be seen in the image below. 

’471 Patent Claim Language	Accused Instrumentality
14. The method according to claim 13, wherein the one or more prompts are ovals on the screen within which the face of the user is placed to capture the at least one first image and the at least one second image.	As explained above, during face data capture the Accused Instrumentality prompts the user to position their face at least two distances from the camera, during which the Accused Instrumentality collects at least two images of the user’s face. These at least two images are collected at different distances between the user’s face and the device camera. As explained above, the Accused Instrumentality utilizes on-screen prompts, including on-screen ovals, to direct the user to adjust the distance between the device and the user so that the user’s face is framed within an “oval” provided on the device’s screen.
15. The method according to claim 10, wherein the computing device is a hand-held device, and the user holds the device at the first and second distances to capture the at least one first image and the at least one second image.	The Accused Instrumentality uses images of a user's face captured using a camera-equipped computing device (e.g., a camera-equipped smartphone, computer, or tablet) to attempt to verify one or more user characteristics and thereby verify the physical presence of the user. *See* www.iproov.com/iproov-system/technology/liveness-assurance; In addition, the Accused Instrumentality “[w]orks on mobile devices, computers, or unattended kiosks.” www.iproov.com/what-we-do/use-cases/authentication. The method may thus be performed on a handheld device where the user holds the computing device at the first distance and then at a second distance to capture the at least one first image and the at least one second image.

16. The method according to claim 10, wherein the first data and the second data comprise biometric data.	As explained above with respect to Claim 10, the iProov server receives from the user's device "biometric data," which is comprised of or based on the user's face images captured by the Accused Instrumentality using the device's camera, including biometric data comprised of or based on the at least one first image of the user's face and biometric data comprised of or based on the at least one second image of the user's face.  **Fig. 2: The Data Controller is iProov's Customer, iProov is the Data Processor** iProov explains how the Accused Instrumentality uses the user's captured biometric data for enrollment and face matching / recognition / verification. ***Enrollment:*** The process of collecting a user's biometric data for the first time. The data is encrypted and sent to a server, binding a verified identity with a biometric to a legitimate account or service. ***Face matching:*** Comparing one face to another to confirm it is the right person. During enrollment a biometric face capture is compared to a photo on an identity document. During authentication the captured biometric data is compared to a previously enrolled biometric template.

’471 Patent Claim Language	Accused Instrumentality
	Face recognition: Technology that matches face biometric data of a user, or users, against an image or database of legitimate information. Typically used as part of a user verification process. ***Face verification:*** Matching the biometric data of the subject user to the biometric data of the expected user. *See* docs.iproov.com/docs/Content/Glossary/iproov-glossary.htm
17. The method according to claim 10, wherein the first data and the second data comprise a mapping of facial features.	FaceTec cannot determine whether the Accused Instrumentality infringes this claim until FaceTec obtains discovery regarding certain non-public aspects of iProov’s verification technology.
18. The method according to claim 10, further comprising displaying an image on a screen of the computing device while capturing the at least one first image and/or the at least one second image, and processing the at least one first image and/or the at least one second image to detect a reflection of the displayed image off of the user's face.	FaceTec cannot determine whether the Accused Instrumentality infringes this claim until FaceTec obtains discovery regarding certain non-public aspects of iProov’s verification technology.

19. The method according to claim 10, wherein the user's face is held steady and the camera moves from the first location to the second location.	The Accused Instrumentality uses images of a user's face captured using a camera-equipped computing device (e.g., a camera-equipped smartphone, computer, or tablet) to attempt to verify one or more user characteristics and thereby verify the physical presence of the user. *See* www.iproov.com/iproov-system/technology/liveness-assurance; In addition, the Accused Instrumentality "[w]orks on mobile devices, computers, or unattended kiosks." www.iproov.com/what-we-do/use-cases/authentication. The method may thus be performed on a handheld device where the user holds the computing device at the first distance and then at a second distance to capture the at least one first image and the at least one second image. In such applications, the user will hold the mobile device at the first and second distances (while holding their face still) to capture the at least one first image and the at least one second image. For example, as shown below FaceTec tested the Accused Instrumentality and performed the claimed steps while moving only the camera relative to the user's face. 

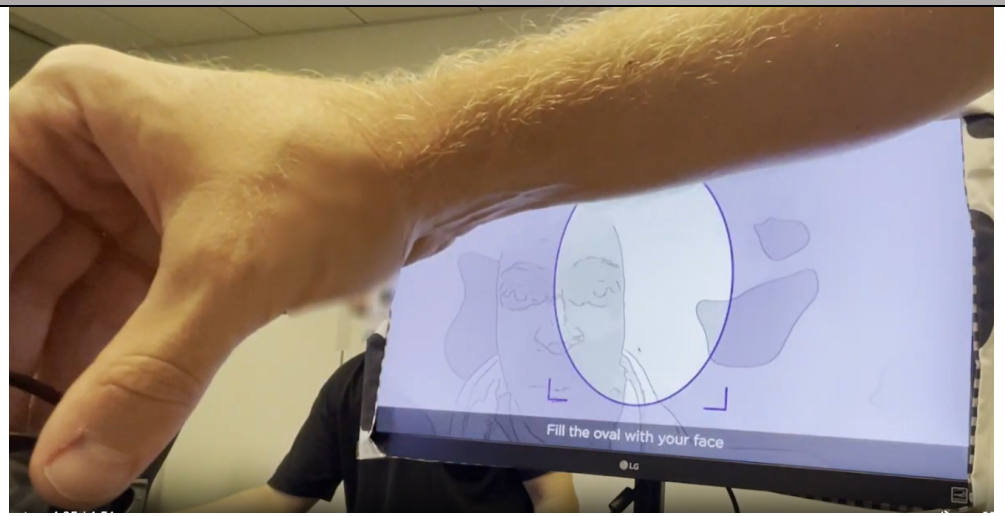
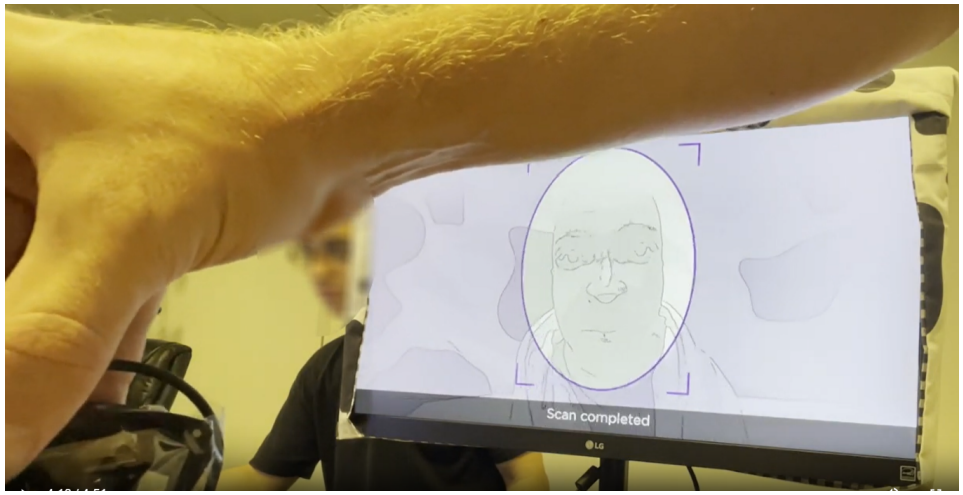
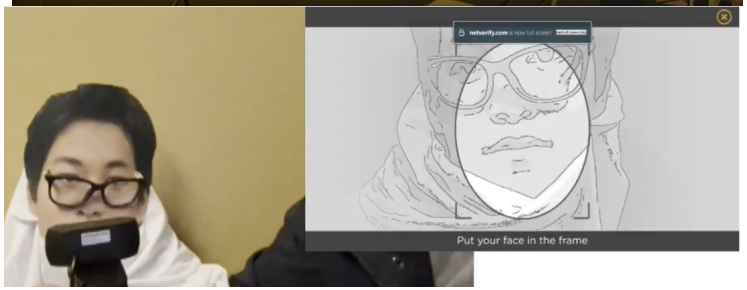
’471 Patent Claim Language	Accused Instrumentality
	 
20. The method according to claim 10, wherein the first data and the second data are maintained on the computing device.	FaceTec cannot determine whether the Accused Instrumentality infringes this claim until FaceTec obtains discovery regarding certain non-public aspects of iProov’s verification technology.

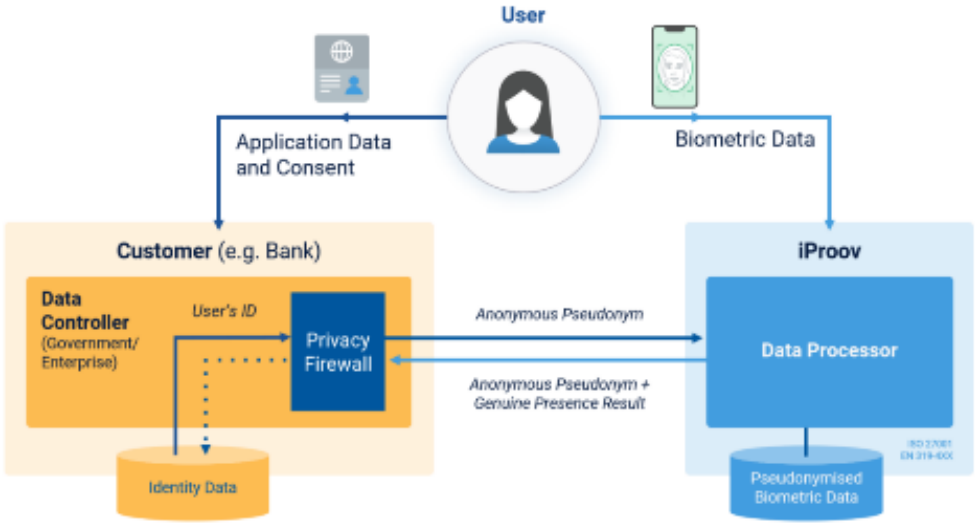
EXHIBIT B

Exhibit B: FaceTec U.S. Pat. 11,157,606 B2

'606 Patent Claim Language	Accused Instrumentality
1. A method for verifying three-dimensionality of a user's face using images of the user's face captured using a camera-equipped computing device, the method comprising:	The Accused Instrumentality uses images of a user's face captured using a camera-equipped computing device (e.g., a camera-equipped smartphone, computer, or tablet) to attempt to verify one or more user characteristics and thereby verify the physical presence of the user. *See* www.iproov.com/iproov-system/technology/liveness-assurance. One aspect that the Accused Instrumentality verifies is three-dimensionality of the user's face as compared to, for example, a two-dimensional photograph. www.iproov.com/videos/liveness-assurance (the Accused Instrumentality confirms that a user is "a real person … [and] not a photograph.")

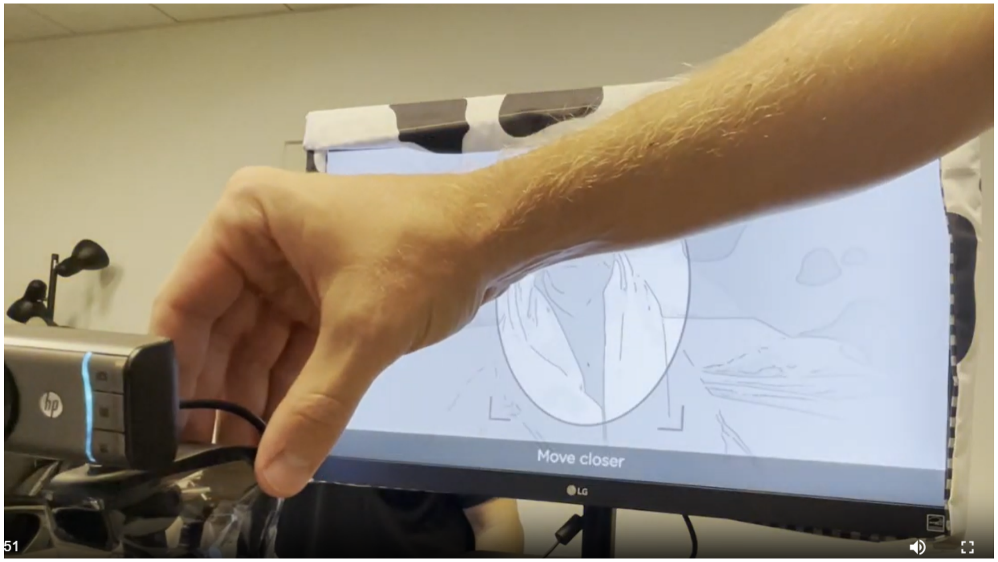
’606 Patent Claim Language	Accused Instrumentality
capturing at least one first image of the user taken with the camera of the computing device at a first distance from the user;	During face data capture the Accused Instrumentality prompts the user to position their face at at least two distances from the camera, during which the Accused Instrumentality collects at least two images of the user’s face. These at least two images are collected at different distances between the user’s face and the device camera. The following images are taken from actual Liveness Assurance authentication sessions. Using a combination of on screen prompts and manipulation of the video shown in the background, the Accused Instrumentality induces the user to change the distance between the device and the user so that images of the user's face are captured at two distances. For example, the Accused Instrumentality manipulates the user to change the distance between the device and the user so that the user’s face is framed within the “oval” provided on the device’s screen. 1. As shown below, the system prompts the user to “put your face in the frame.”   2. After the user frames their face in the oval, the Accused Instrumentality captures at least one image of the user, which image is taken at a first distance. *See* www.iproov.com/what-we-do/use-cases/authentication

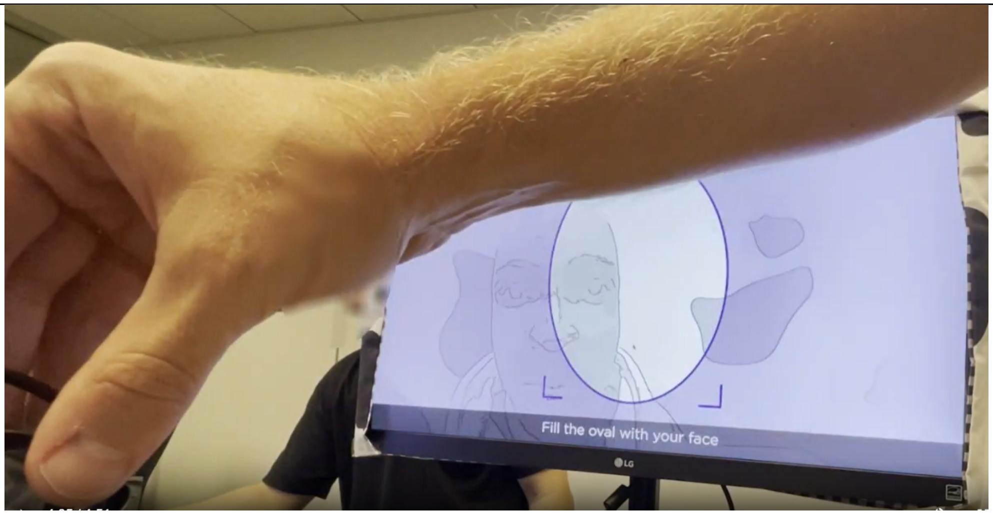
processing the at least one first image to obtain first biometric data from the at least one first image;	During the image capture process described herein, the Accused Instrumentality typically captures approximately 10 image frames of the user. The Accused Instrumentality packages these images into a "WebM payload," which the user's device then sends to iProov's server for data processing. Using the publicly available Chrome Dev Tools Network Tab (developer.chrome.com/docs/devtools/network/), one can examine the contents of this WebM payload, which the Accused Instrumentality sends in unencrypted format. Below are several image frames taken from the WebM payload filed created during a Liveness Assurance authentication session. As can be seen, image frames are collected at a different distance between the user and the camera:  *See also* docs.iproov.com/docs/Content/ImplementationGuide/api/api-optional-features.htm ("You can optionally request the image of the user that is captured during an enroll validate or claim validate process. The following frame will be provided in the API response: LA: last frame [and] GPA: 4th frame.")

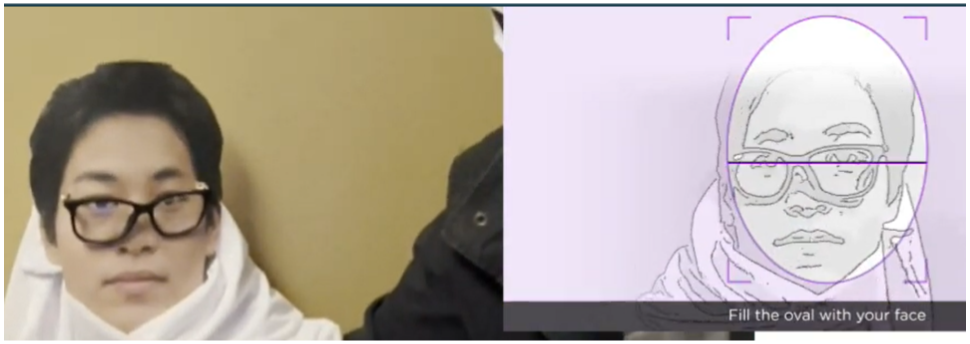
	As shown in iProov's data flow chart below, the iProov server receives from the user's device this WebM payload, which includes "biometric data," including "first data" comprised of or based on the user's face captured by the Accused Instrumentality and at least one other image of the user's face captured at a different distance.  **Fig. 2: The Data Controller is iProov's Customer, iProov is the Data Processor** iProov explains how the Accused Instrumentality uses the user's captured biometric data for enrollment and face matching / recognition / verification. ***Enrollment:*** The process of collecting a user's biometric data for the first time. The data is encrypted and sent to a server, binding a verified identity with a biometric to a legitimate account or service. ***Face matching:*** Comparing one face to another to confirm it is the right person. During enrollment a biometric face capture is compared to a photo on an identity document. During authentication the captured biometric data is compared to a previously enrolled biometric template. ***Face recognition:*** Technology that matches face biometric data of a user, or users, against an image or database of legitimate information. Typically used as part of a user verification process.

Case 2:24-cv-02526-RFB-NW Document 1-9-6 Filed 04/19/24 Page 42 of 78

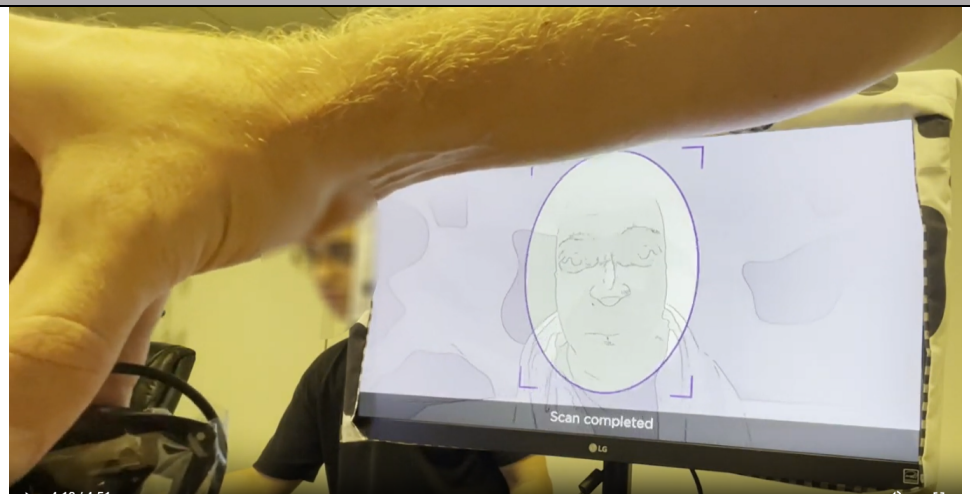
’606 Patent Claim Language	Accused Instrumentality
	Face verification: Matching the biometric data of the subject user to the biometric data of the expected user. *See* docs.iproov.com/docs/Content/Glossary/iproov-glossary.htm

capturing at least one second image of the user taken with the camera of the computing device at a second distance from the user, the second distance being different than the first distance;	During face data capture the Accused Instrumentality prompts the user to position their face at least two distances from the camera, during which the Accused Instrumentality collects at least two images of the user's face. These at least two images are collected at different distances between the user's face and the device camera. 3. After capturing the at least one first image of the user's face (described above), the system changes the visible background resolution and instructs the user to "move closer" and to "fill the oval with your face." This can be seen in the images below: 

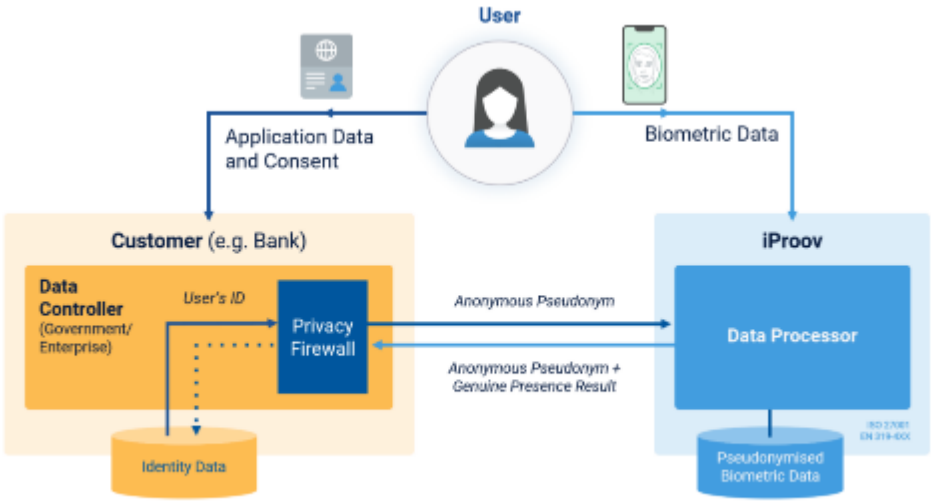




4. As the user changes the distance between their face and the camera as a result of the prompts so as to fill the oval with their face, the camera captures multiple additional images of the user, including at least one second image at a second distance different from the first distance.
5. After capturing the at least one first and second images of the user, the Accused Instrumentality then displays to the user "scan completed." This can be seen in the image below.

’606 Patent Claim Language	Accused Instrumentality
	

processing the at least one second image to obtain second biometric data based on the at least one second image;	During the image capture process described herein, the Accused Instrumentality captures approximately 10 image frames of the user. The Accused Instrumentality packages these images into a "WebM payload," which the user's device then to iProov's server for data processing. Using the publicly available Chrome Dev Tools Network Tab (developer.chrome.com/docs/devtools/network/), one can easily examine the contents of this WebM payload, which the Accused Instrumentality sends in unencrypted format. Below are several image frames taken from the WebM payload filed created during a Liveness Assurance authentication session. As can be seen, image frames are collected at a different distance between the user and the device camera:  *See also* docs.iproov.com/docs/Content/ImplementationGuide/api/api-optional-features.htm ("You can optionally request the image of the user that is captured during an enroll validate or claim validate process. The following frame will be provided in the API response: LA: last frame [and] GPA: 4th frame.")

	As shown in iProov's data flow chart below, the iProov server receives from the user's device this WebM payload, which includes "biometric data" containing the "first data" and including "second data" comprised of or based on the at least one second image of the user's face captured by the Accused Instrumentality.  **Fig. 2: The Data Controller is iProov's Customer, iProov is the Data Processor** iProov explains how the Accused Instrumentality uses the user's captured biometric data for enrollment and face matching / recognition / verification. ***Enrollment:*** The process of collecting a user's biometric data for the first time. The data is encrypted and sent to a server, binding a verified identity with a biometric to a legitimate account or service. ***Face matching:*** Comparing one face to another to confirm it is the right person. During enrollment a biometric face capture is compared to a photo on an identity document. During authentication the captured biometric data is compared to a previously enrolled biometric template. ***Face recognition:*** Technology that matches face biometric data of a user, or users, against an image or database of legitimate information. Typically used as part of a user verification process.

’606 Patent Claim Language	Accused Instrumentality
	Face verification: Matching the biometric data of the subject user to the biometric data of the expected user. *See* https://docs.iproov.com/docs/Content/Glossary/iproov-glossary.htm

comparing the first biometric data with the second biometric data to determine whether the first biometric data matches the second biometric data;	The iProov Server receives biometric information regarding the user, including the first biometric data and the second biometric data discussed above. iProov has confirmed that the Accused Instrumentality operates using a neural network ("iProov Neural Network"). > "By default, the technology picks up certain cues on the face to detect that it is actually human. This uses technology that learns on an ongoing, continuous basis. So, the solution deploys deep convolutional neural network and computer vision technology, which uses machine learning algorithms. Thus, the idea is that more people can authenticate themselves. The person goes through the authentication process; the algorithm learns to understand the behavior of the human face based on how the person's features change over time or how they respond while looking at the screen. This is how iProov uses deep learning technology in our biometric product." https://itsecuritywire.com/interviews/remote-identification-process-simplified-and-safeguarded-by-the-biometr; *see also* https://docs.iproov.com/docs/Content/Overview/biometric-assurance.htm ("Liveness Assurance is a patented 3D passive face biometric verification technology that combines camera imagery and contextual data from the authentication process. Powerful deep learning AI methods assure accurate face matching and determine liveness."); **Liveness Assurance** Liveness Assurance is a patented 3D passive face biometric verification technology that combines camera imagery and contextual data from the authentication process. Powerful deep learning AI methods assure accurate face matching and determine liveness. LA has these benefits: • Delivers a simple, passive, and low ceremony user experience. • Provides assurance it's a **real** person and the **right** person. • Defends against known digital or physical presentation attacks and camera bypass digital attacks.

’606 Patent Claim Language	Accused Instrumentality
	The iProov Neural Network necessarily analyzes all data provided to it to verify to a high level of confidence that the user is three-dimensional. www.iproov.com/videos/liveness-assurance (the Accused Instrumentality confirms that a user is “a real person … [and] not a photograph.”). The iProov Neural Network verifies this based at least in part on analyzing the first data and the second data. The iProov Neural Network internally compares the first data and the second data to identify similarities and differences therebetween. This comparison includes (1) whether the first biometric data has differences from the second biometric data, and (2) whether the differences between the first biometric data and the second biometric data match expected differences between an image of a three-dimensional user’s face taken at the first distance and an image of a user’s three-dimensional face taken at the second distance. *See, e.g.*, IP-00003260; *see also* IP-00003256-61. The Accused Instrumentality requires no change (facial or otherwise) other than a change in distance (and potentially face realignment within the oval) between the user and the device.

comparing the first biometric data to second biometric data to determine whether differences between the at least one first image and the at least one second image match expected differences resulting from movement of the camera or the user which changed the distance between the user and camera from the first distance to the second distance;	The iProov Server receives biometric information regarding the user, including the first biometric data and the second biometric data discussed above. iProov has confirmed that the Accused Instrumentality operates using a neural network ("iProov Neural Network"). > "By default, the technology picks up certain cues on the face to detect that it is actually human. This uses technology that learns on an ongoing, continuous basis. So, the solution deploys deep convolutional neural network and computer vision technology, which uses machine learning algorithms. Thus, the idea is that more people can authenticate themselves. The person goes through the authentication process; the algorithm learns to understand the behavior of the human face based on how the person's features change over time or how they respond while looking at the screen. This is how iProov uses deep learning technology in our biometric product." https://itsecuritywire.com/interviews/remote-identification-process-simplified-and-safeguarded-by-the-biometr; *see also* https://docs.iproov.com/docs/Content/Overview/biometric-assurance.htm ("Liveness Assurance is a patented 3D passive face biometric verification technology that combines camera imagery and contextual data from the authentication process. Powerful deep learning AI methods assure accurate face matching and determine liveness."); **Liveness Assurance** Liveness Assurance is a patented 3D passive face biometric verification technology that combines camera imagery and contextual data from the authentication process. Powerful deep learning AI methods assure accurate face matching and determine liveness. LA has these benefits: • Delivers a simple, passive, and low ceremony user experience. • Provides assurance it's a **real** person and the **right** person. • Defends against known digital or physical presentation attacks and camera bypass digital attacks.

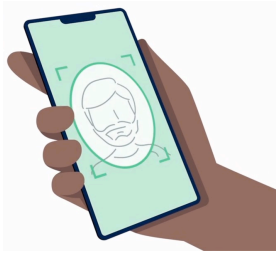
’606 Patent Claim Language	Accused Instrumentality
	The iProov Neural Network necessarily analyzes all data provided to it to verify to a high level of confidence that the user is three-dimensional. www.iproov.com/videos/liveness-assurance (the Accused Instrumentality confirms that a user is “a real person … [and] not a photograph.”). The iProov Neural Network verifies this based at least in part on analyzing the first biometric data and the second biometric data. The iProov Neural Network internally compares the first biometric data and the second biometric data to identify similarities and differences therebetween. This comparison includes (1) whether the first biometric data has differences from the second biometric data, and (2) whether the differences between the first biometric data and the second biometric data match expected differences between an image of a three-dimensional user’s face taken at the first distance and an image of a user’s three-dimensional face taken at the second distance. *See, e.g.*, IP-00003260; *see also* IP-00003256-61. The Accused Instrumentality requires no change (facial or otherwise) other than a change in distance (and potentially face realignment within the oval) between the user and the device.”

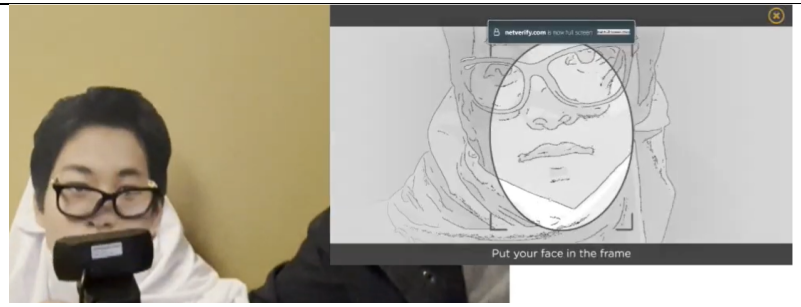
determining that the user's face is three-dimensional when: the first biometric data does not match the second biometric data; and the second biometric data has the expected differences as compared to the first biometric data resulting from the change in distance between the user and the camera when capturing the at least one first image and the at least one second image.	As shown in the images reproduced above, the Accused Instrumentality necessarily requires that the first biometric data is not identical to the second biometric data. For example, the images below each necessarily have different biometric data:  In addition, unless expected differences between the first biometric data and the second biometric data are observed by the iProov Neural Network, the Accused Instrumentality normally will not confirm that the user is physically present. For example, the Accused Instrumentality will normally not confirm the user is physically present when a two-dimensional photo is used in a "spoof" attempt. *See*, e.g., www.iproov.com/videos/liveness-assurance (the Accused Instrumentality confirms that a user is "a real person … [and] not a photograph.") *See also* IP-00003256-61. Conversely, FaceTec has tested the Accused Instrumentality and confirmed that if expected distortion between the first data and the second data matches expected distortion between an image of a user's three-dimensional face taken at the first distance and an image of a user's three-dimensional face taken at the second distance, the Accused Instrumentality will normally confirm the user's face is three-dimensional and that the user is likely to be physically present. For example, FaceTec tested the Accused Instrumentality and confirmed that Accused Instrumentality will

Case 3:24-cv-00226-AR-RLW Document 89-6 Filed 04/29/24 Page 54 of 78

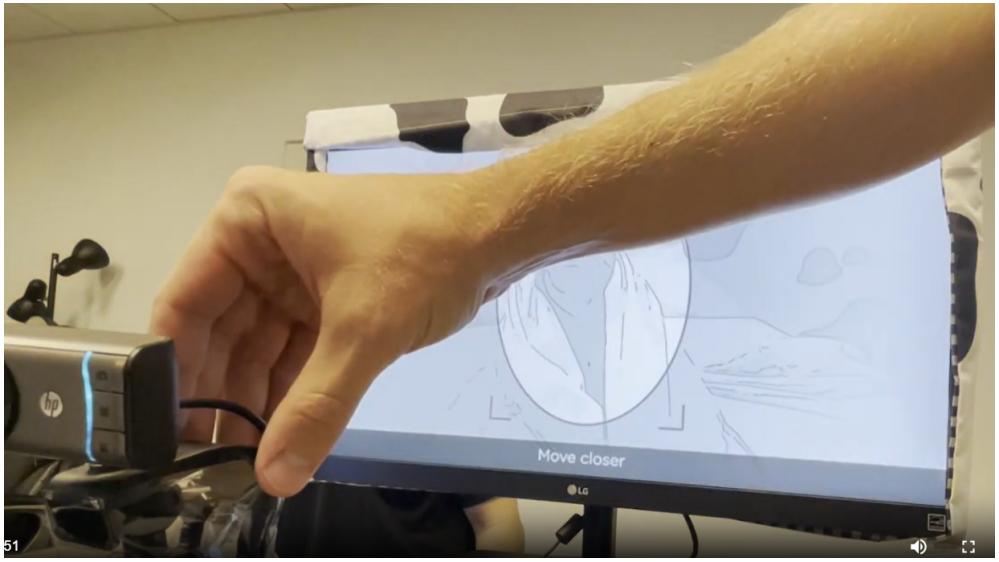
’606 Patent Claim Language	Accused Instrumentality
	normally confirm the user is physically present when a three-dimensional user conducts the verification steps outlined above. As shown in the images reproduced above, FaceTec tested the Accused Instrumentality using both a three dimensional “doll” head as well as a two-dimensional photo that had been modified with both a shawl and a pair of eyeglasses, both of which the Accused Instrumentality successfully verified.
2. The method according to claim 1, further comprising: interpolating the first biometric data and the second biometric data to obtain estimated intermediate biometric data; capturing at least one third image of the user taken with the camera of the computing device at a third distance from the user, the third distance being between the first distance and the second distance; processing the at least one third image to obtain third biometric data based on the at least one third image; and comparing the estimated intermediate biometric data with the third biometric data to determine whether the third biometric data matches the estimated intermediate biometric data.	FaceTec cannot determine whether iProov infringes this claim until FaceTec obtains discovery regarding certain non-public aspects of iProov’s verification technology.

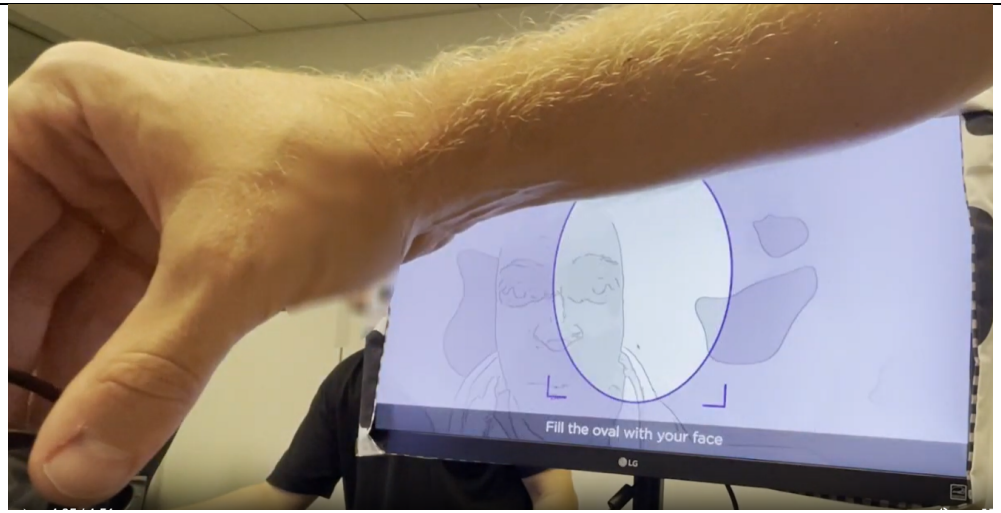
’606 Patent Claim Language	Accused Instrumentality
3. The method according to claim 1, further comprising verifying the presence of the user's ears in the at least one first image, and verifying the absence or reduced visibility of the user's ears in the at least one second image, wherein the first distance is larger than the second distance.	FaceTec cannot determine whether iProov infringes this claim until FaceTec obtains discovery regarding certain non-public aspects of iProov’s verification technology.

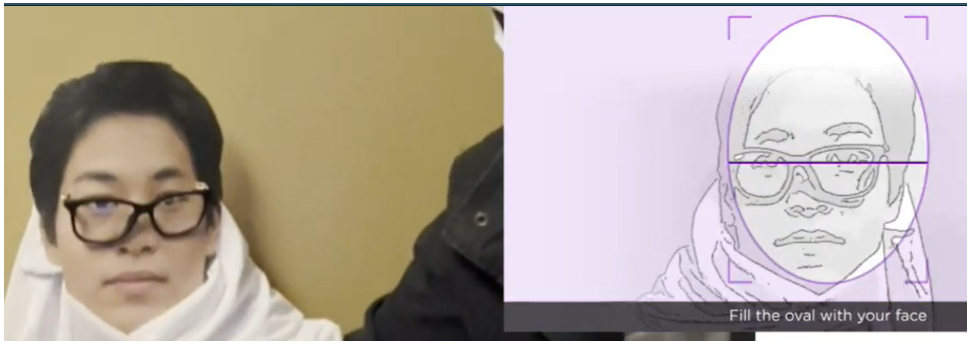
4. The method according to claim 1, wherein the computing device is configured to display one or more prompts on a screen of the computing device to guide the user to capture the at least one first image at the first distance and the at least on second image at the second distance.	During face data capture the Accused Instrumentality prompts the user to position their face at at least two distances from the camera, during which the Accused Instrumentality collects at least two images of the user's face. These at least two images are collected at different distances between the user's face and the device camera. Using on-screen prompts, the Accused Instrumentality directs the user to adjust the distance between the camera and the user so that the user's face is framed within an "oval" provided on the device's screen.  *See* www.iproov.com/what-we-do/use-cases/authentication The following images are taken from actual Liveness Assurance authentication sessions. Using a combination of on screen prompts and manipulation of the video shown in the background, the Accused Instrumentality induces the user to change the distance between the device and the user so that images of the user's face are captured at two distances. For example, the Accused Instrumentality manipulates the user to change the distance between the device and the user so that the user's face is framed within the "oval" provided on the device's screen. 1. As shown below, the system prompts the user to "put your face in the frame." 



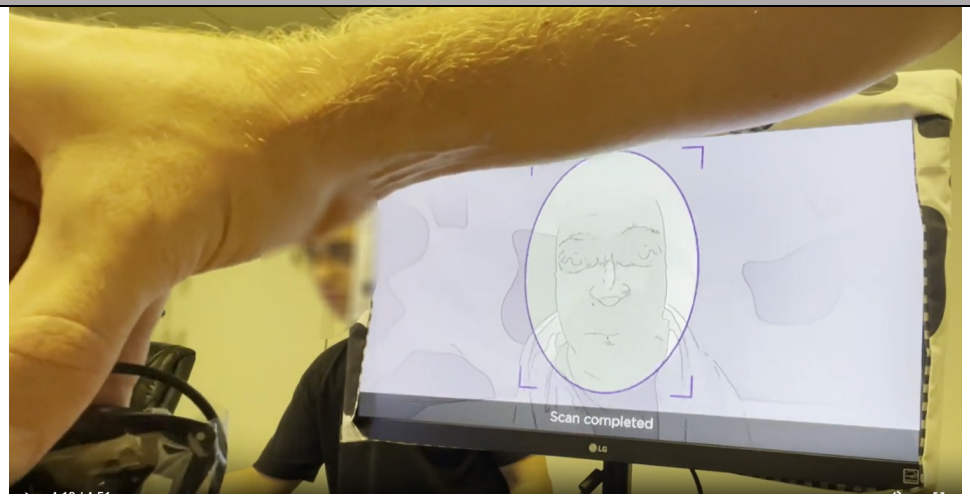
2. After the user frames their face in the oval, the Accused Instrumentality captures at least one image of the user, which image is taken at a first distance.
3. After capturing the at least one first image of the user's face (described above), the system changes the background resolution that is displayed and prompts the user to "move closer" and to "fill the oval with your face." This can be seen in the images below:

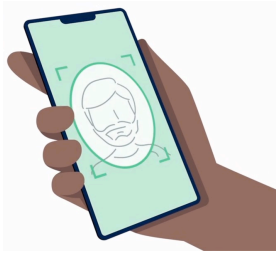


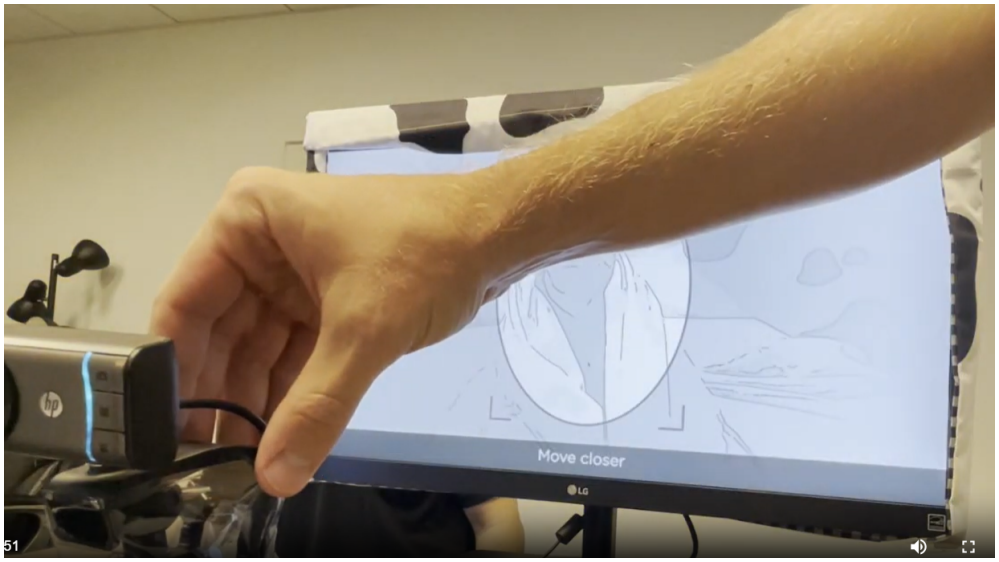


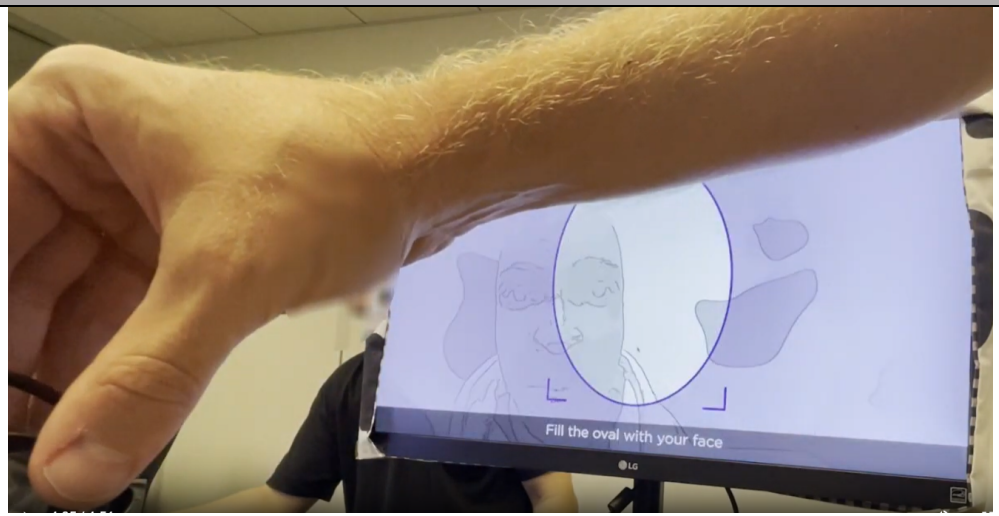
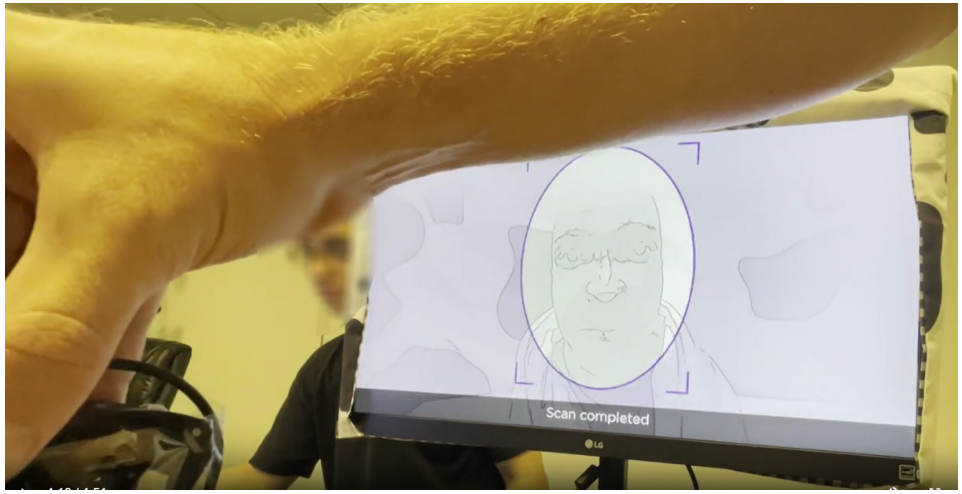


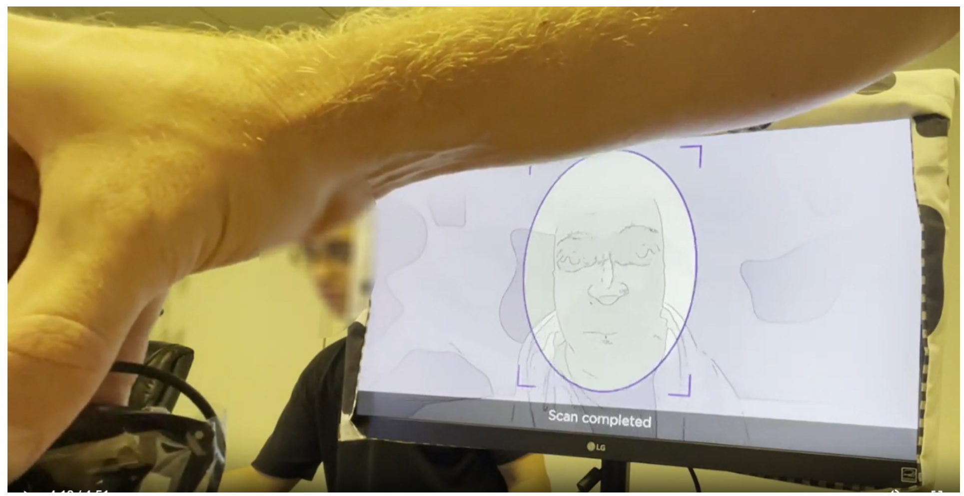
4. As the user changes the distance between their face and the camera so as to fill the oval with their face, the camera captures multiple additional images of the user, including at least one second image that is captured at a second distance different from the first distance.
5. After capturing the at least one first and second images of the user, the Accused Instrumentality then displays to the user “scan completed.” This can be seen in the image below.

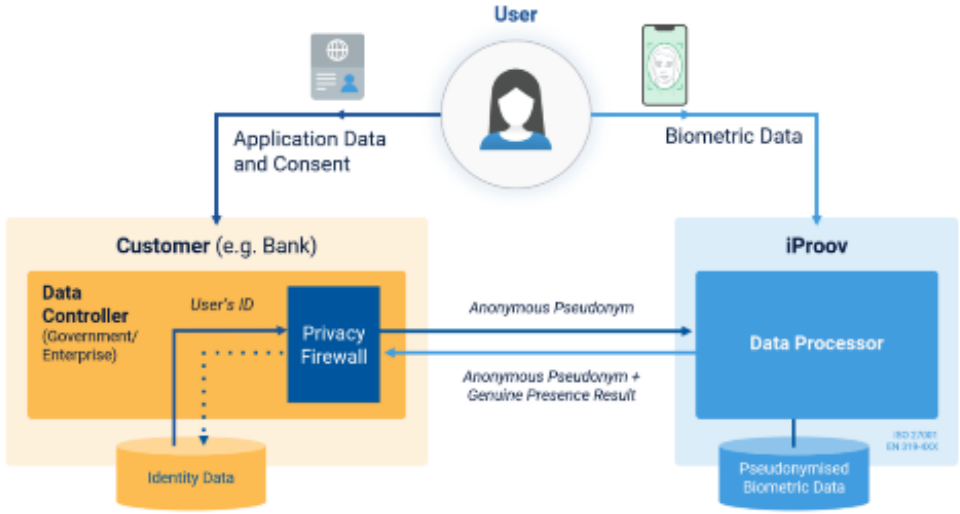
’606 Patent Claim Language	Accused Instrumentality
	

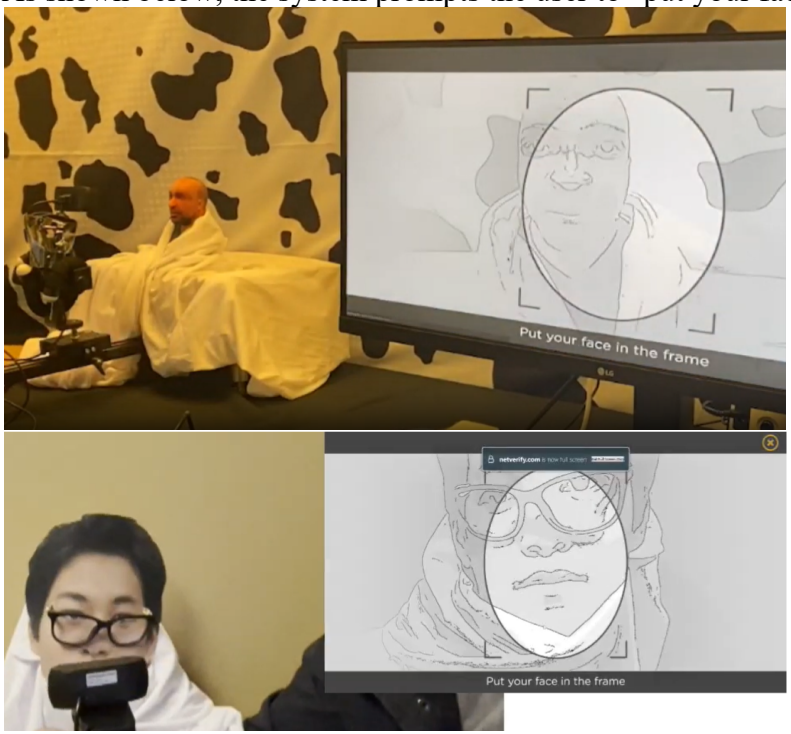
'606 Patent Claim Language	Accused Instrumentality
5. The method according to claim 4, wherein the one or more prompts are ovals sized on the screen within which the face of the user is placed to capture the at least one first image and the at least one second image at the first and second distances.	As explained above, during face data capture the Accused Instrumentality prompts the user to position their face at least two distances from the camera, during which the Accused Instrumentality collects at least two images of the user's face. These at least two images are collected at different distances between the user's face and the device camera. As explained above, the Accused Instrumentality utilizes on-screen prompts, including on-screen ovals, to direct the user to adjust the distance between the device and the user so that the user's face is framed within an "oval" provided on the device's screen.  *See* www.iproov.com/what-we-do/use-cases/authentication As the user alters the distance between their face and the device so as to remain framed within the oval, the Accused Instrumentality captures at least two images of the user's face, including at least one first image of the user taken with the camera of the computing device at a first distance from the user and at least one second image of the user taken with the camera of the computing device at a second distance from the user.

6. The method according to claim 4, wherein the computing device is a hand-held device, and the user holds the computing device at the first distance and the second distance to capture the at least one first image and the at least one second image.	The Accused Instrumentality uses images of a user's face captured using a camera-equipped computing device (e.g., a camera-equipped smartphone, computer, or tablet) to attempt to verify one or more user characteristics and thereby verify the physical presence of the user. *See* www.iproov.com/iproov-system/technology/liveness-assurance; In addition, the Accused Instrumentality "[w]orks on mobile devices, computers, or unattended kiosks." www.iproov.com/what-we-do/use-cases/authentication. The method may thus be performed on a handheld device where the user holds the computing device at the first distance and then at a second distance to capture the at least one first image and the at least one second image. For example, as shown below FaceTec tested the Accused Instrumentality and performed the claimed steps while moving only the camera relative to the user's face. 

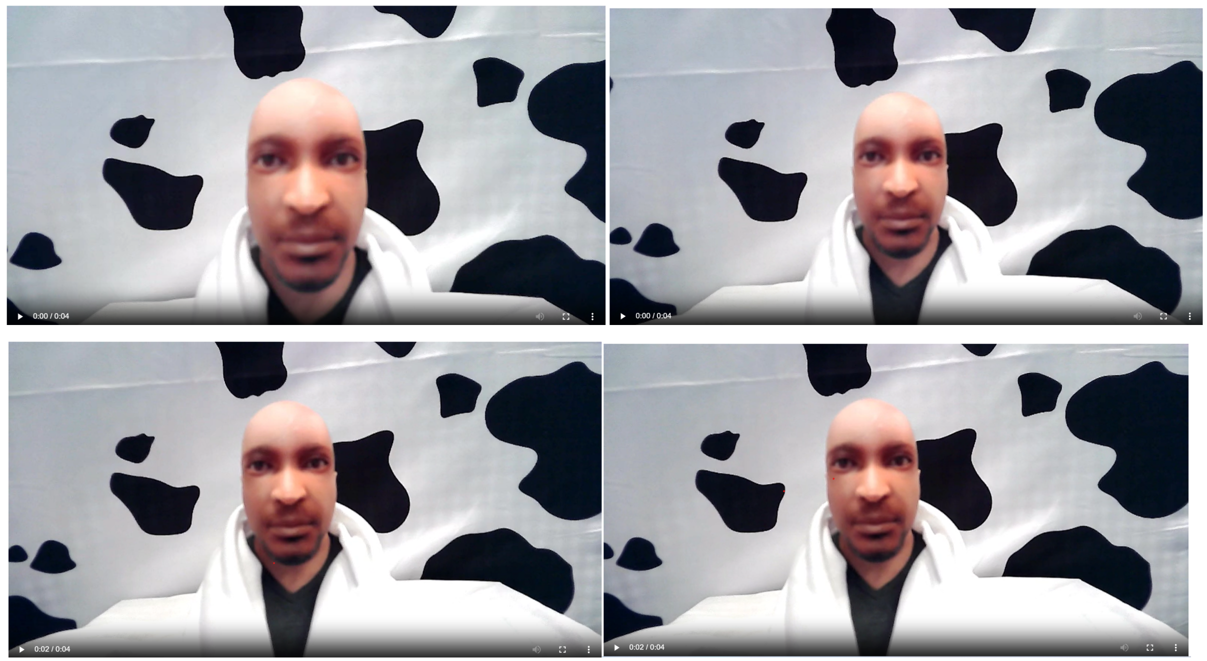
’606 Patent Claim Language	Accused Instrumentality
	 

’606 Patent Claim Language	Accused Instrumentality
7. The method according to claim 6, wherein the computing device comprises a laptop or desktop computer and, with the computing device stationary, the user moves from the first distance to the second distance to capture the at least one first image and the at least one second image.	The Accused Instrumentality uses images of a user's face captured using a camera-equipped computing device (e.g., a camera-equipped smartphone, computer, or tablet) to attempt to verify one or more user characteristics and thereby verify the physical presence of the user. *See* www.iproov.com/iproov-system/technology/liveness-assurance; In addition, the Accused Instrumentality “[w]orks on mobile devices, computers, or unattended kiosks.” www.iproov.com/what-we-do/use-cases/authentication. The method may thus be performed on a laptop or desktop computer where the user moves their face from the first distance to the second distance and the Accused Instrumentality captures the at least one first image and the at least one second image.
8. The method according to claim 1, further comprising displaying an image on a screen of the computing device while capturing the at least one first and/or the at least one second image.	As shown in the images reproduced above, the Accused Instrumentality displays an image representing the user’s head/face on a screen of the device while capturing the at least one first and the at least one second image. For example: 

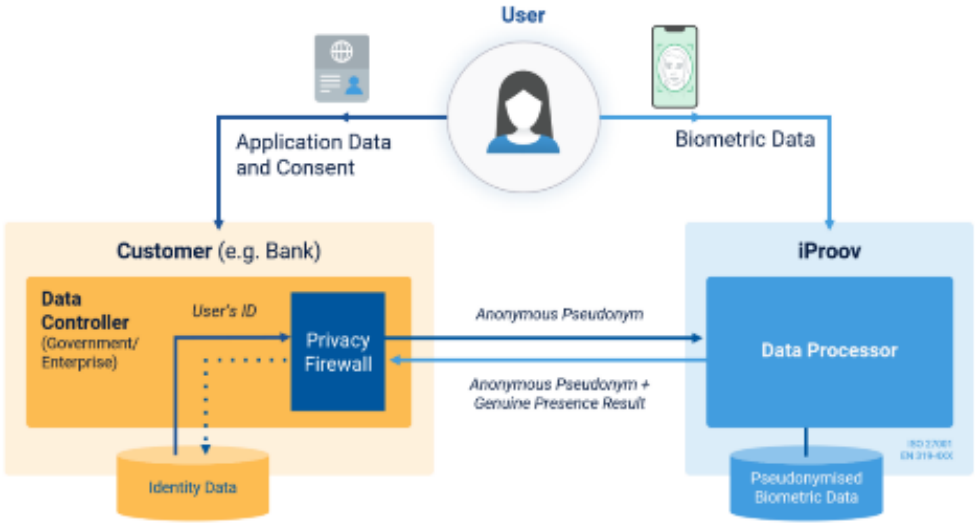
'606 Patent Claim Language	Accused Instrumentality
9. The method according to claim 1, wherein the first biometric data and the second biometric data are transmitted over a network to a server.	As explained above with respect to Claim 1, the iProov server receives from the user's device "biometric data," which is comprised of or based on the user's face images captured by the Accused Instrumentality. This server receives this information over a network. *See* www.iproov.com/blog/cloud-biometrics-vs-on-device-difference ("At iProov, we believe that cloud-based, or server-side, biometric authentication is the only option to securely authenticate users remotely. If you use iProov, you are buying a cloud-hosted solution. … The entire authentication process happens server-side, independently from the device.")  **Fig. 2: The Data Controller is iProov's Customer, iProov is the Data Processor**
19. A method for verifying three-dimensionality of a user's face using images of the user's face captured using a camera-equipped computing device, the method comprising:	The Accused Instrumentality uses images of the user's face captured using a camera-equipped computing device (e.g., a camera-equipped smartphone, computer, or tablet) to attempt to verify one or more user characteristics and thereby verify the physical presence of a user. *See* www.iproov.com/iproov-system/technology/liveness-assurance. One aspect that the Accused Instrumentality verifies is three-dimensionality of the user's face, as compared to, for example, a two-dimensional photograph. www.iproov.com/videos/liveness-assurance (the Accused Instrumentality confirms that a user is "a real person … [and] not a photograph.")

receiving first biometric data generated from at least one first image of the user taken with the camera of the computing device located at a first distance from the user;	During face data capture the Accused Instrumentality prompts the user to position their face at at least two distances from the camera, during which the Accused Instrumentality collects at least two images of the user's face. These at least two images are collected at different distances between the user's face and the device camera. The following images are taken from actual Liveness Assurance authentication sessions. Using a combination of on screen prompts and manipulation of the video shown in the background, the Accused Instrumentality induces the user to change the distance between the device and the user so that images of the user's face are captured at two distances. For example, the Accused Instrumentality manipulates the user to change the distance between the device and the user so that the user's face is framed within the "oval" provided on the device's screen. 1. As shown below, the system prompts the user to "put your face in the frame."  2. After the user frames their face in the oval, the Accused Instrumentality captures at least one image of the user, which image is taken at a first distance. *See* www.iproov.com/what-we-do/use-cases/authentication

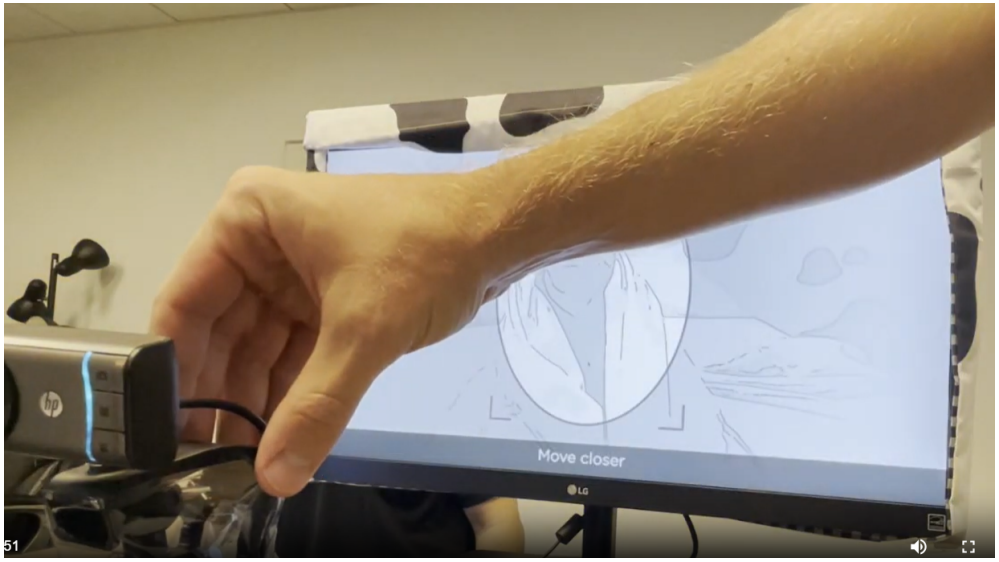
During the image capture process described herein, the Accused Instrumentality typically captures approximately 10 image frames of the user. The Accused Instrumentality packages these images into a "WebM payload," which the user's device then sends to iProov's server for data processing. Using the publicly available Chrome Dev Tools Network Tab (developer.chrome.com/docs/devtools/network/), one can examine the contents of this WebM payload, which the Accused Instrumentality sends in unencrypted format. Below are several image frames taken from the WebM payload filed created during a Liveness Assurance authentication session. As can be seen, image frames are collected at a different distance between the user and the camera:

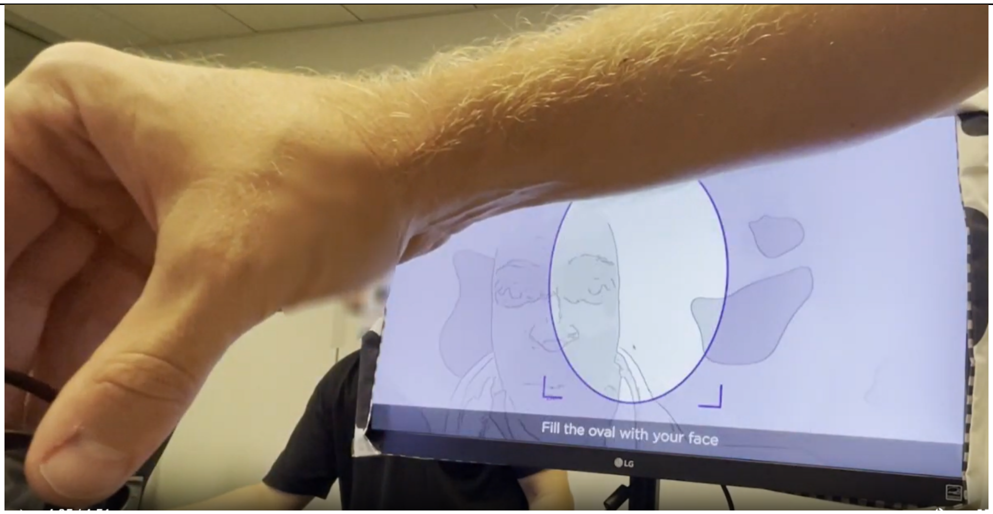
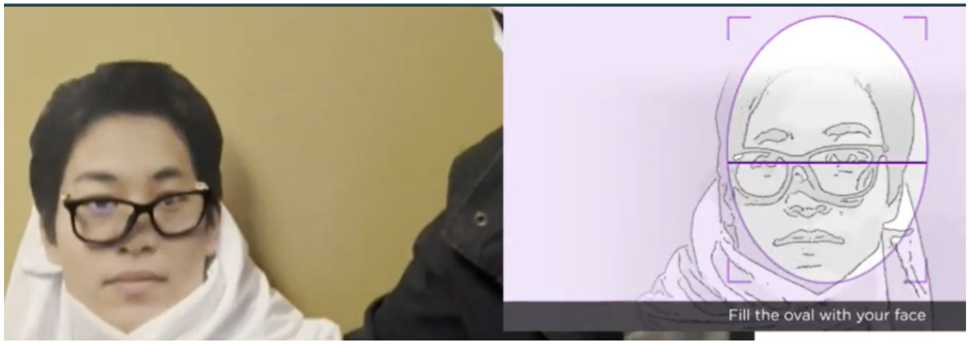


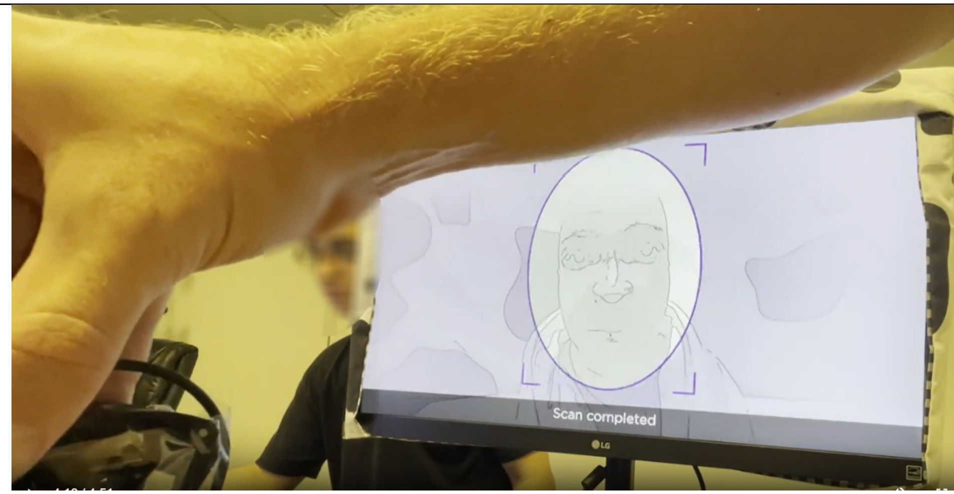
See also docs.iproov.com/docs/Content/ImplementationGuide/api/api-optional-features.htm ("You can optionally request the image of the user that is captured during an enroll validate or claim validate process. The following frame will be provided in the API response: LA: last frame [and] GPA: 4th frame.")

	As shown in iProov's data flow chart below, the iProov server receives from the user's device this WebM payload, which includes "biometric data," including "first data" comprised of or based on the user's face captured by the Accused Instrumentality and at least one other image of the user's face captured at a different distance.  **Fig. 2: The Data Controller is iProov's Customer, iProov is the Data Processor** iProov explains how the Accused Instrumentality uses the user's captured biometric data for enrollment and face matching / recognition / verification. ***Enrollment:*** The process of collecting a user's biometric data for the first time. The data is encrypted and sent to a server, binding a verified identity with a biometric to a legitimate account or service. ***Face matching:*** Comparing one face to another to confirm it is the right person. During enrollment a biometric face capture is compared to a photo on an identity document. During authentication the captured biometric data is compared to a previously enrolled biometric template. ***Face recognition:*** Technology that matches face biometric data of a user, or users, against an image or database of legitimate information. Typically used as part of a user verification process.

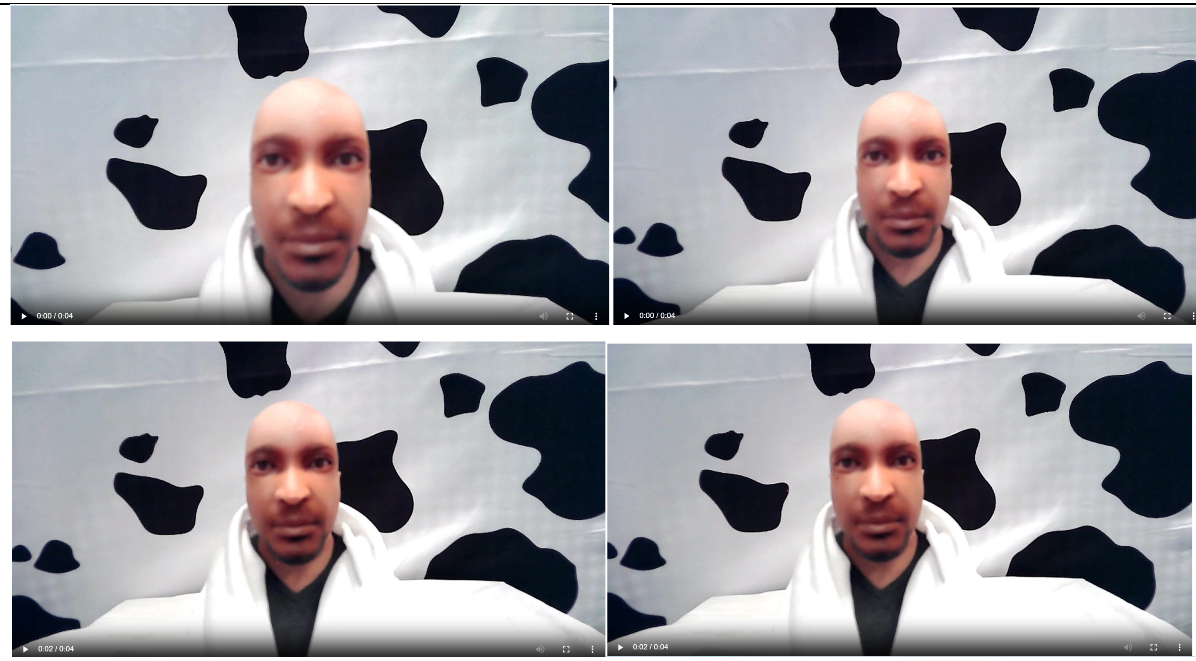
’606 Patent Claim Language	Accused Instrumentality
	Face verification: Matching the biometric data of the subject user to the biometric data of the expected user. *See* docs.iproov.com/docs/Content/Glossary/iproov-glossary.htm

receiving second biometric data generated from at least one second image of the user taken with the camera of the computing device located at a second distance from the user, the second distance being different than the first distance;	During face data capture the Accused Instrumentality prompts the user to position their face at least two distances from the camera, during which the Accused Instrumentality collects at least two images of the user's face. These at least two images are collected at different distances between the user's face and the device camera. 3. After capturing the at least one first image of the user's face (described above), the system changes the visible background resolution and instructs the user to "move closer" and to "fill the oval with your face." This can be seen in the images below: 

	  4. As the user changes the distance between their face and the camera as a result of the prompts so as to fill the oval with their face, the camera captures multiple additional images of the user, including at least one second image at a second distance different from the first distance. 5. After capturing the at least one first and second images of the user, the Accused Instrumentality then displays to the user “scan completed.” This can be seen in the image below.



During the image capture process described herein, the Accused Instrumentality typically captures approximately 10 image frames of the user. The Accused Instrumentality packages these images into a "WebM payload," which the user's device then sends to iProov's server for data processing. Using the publicly available Chrome Dev Tools Network Tab (developer.chrome.com/docs/devtools/network/), one can examine the contents of this WebM payload, which the Accused Instrumentality sends in unencrypted format. Below are several image frames taken from the WebM payload filed created during a Liveness Assurance authentication session. As can be seen, image frames are collected at a different distance between the user and the camera:

	 See also docs.iproov.com/docs/Content/ImplementationGuide/api/api-optional-features.htm ("You can optionally request the image of the user that is captured during an enroll validate or claim validate process. The following frame will be provided in the API response: LA: last frame [and] GPA: 4th frame.") As shown in iProov's data flow chart below, the iProov server receives from the user's device this WebM payload, which includes "biometric data," including "first data" comprised of or based on the user's face captured by the Accused Instrumentality and at least one other image of the user's face captured at a different distance.

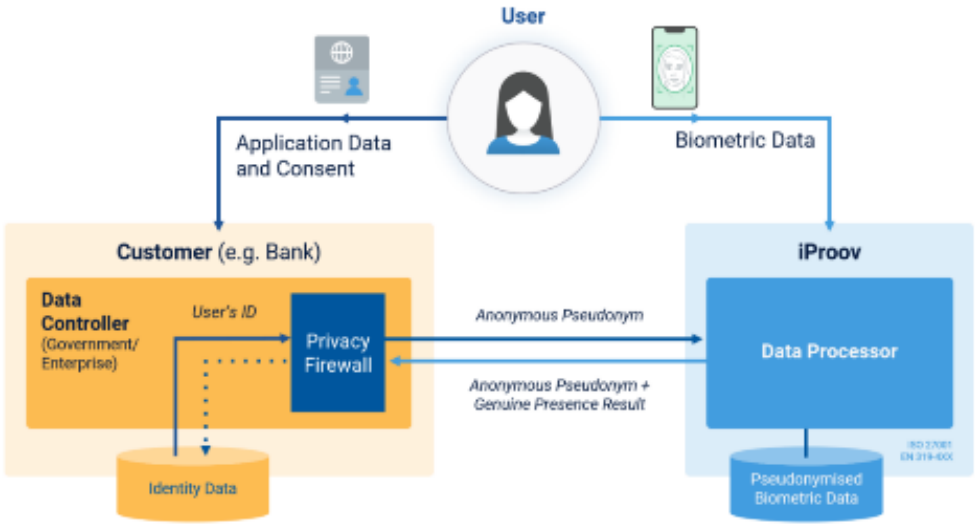


Fig. 2: The Data Controller is iProov's Customer, iProov is the Data Processor

iProov explains how the Accused Instrumentality uses the user's captured biometric data for enrollment and face matching / recognition / verification.

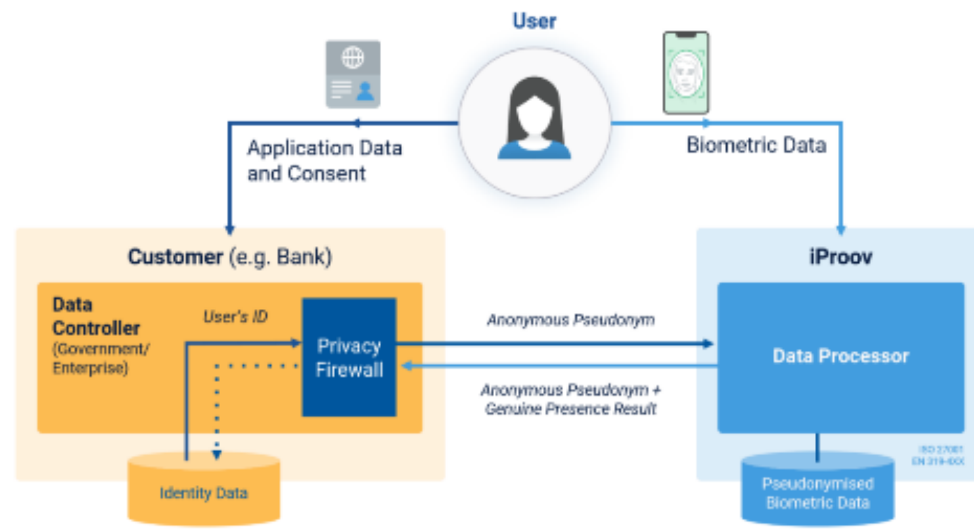
> ***Enrollment:*** The process of collecting a user's biometric data for the first time. The data is encrypted and sent to a server, binding a verified identity with a biometric to a legitimate account or service.
>
> ***Face matching:*** Comparing one face to another to confirm it is the right person. During enrollment a biometric face capture is compared to a photo on an identity document. During authentication the captured biometric data is compared to a previously enrolled biometric template.
>
> ***Face recognition:*** Technology that matches face biometric data of a user, or users, against an image or database of legitimate information. Typically used as part of a user verification process.
>
> ***Face verification:*** Matching the biometric data of the subject user to the biometric data of the expected user.

See docs.iproov.com/docs/Content/Glossary/iproov-glossary.htm

comparing the first biometric data with the second biometric data to determine whether the first biometric data matches the second biometric data; comparing the first biometric data with second biometric data to determine whether differences between the at least one first image and the at least one second image match expected differences resulting from movement of the camera or the user which changes the distance between the user and camera for capture of the one or more first images at the first distance and capture of the one or more second images at the second distance;	The iProov Server receives biometric information regarding the user, including the first biometric data and the second biometric data discussed above. iProov has confirmed that the Accused Instrumentality operates using a neural network ("iProov Neural Network"). > "By default, the technology picks up certain cues on the face to detect that it is actually human. This uses technology that learns on an ongoing, continuous basis. So, the solution deploys deep convolutional neural network and computer vision technology, which uses machine learning algorithms. Thus, the idea is that more people can authenticate themselves. The person goes through the authentication process; the algorithm learns to understand the behavior of the human face based on how the person's features change over time or how they respond while looking at the screen. This is how iProov uses deep learning technology in our biometric product." https://itsecuritywire.com/interviews/remote-identification-process-simplified-and-safeguarded-by-the-biometr; *see also* https://docs.iproov.com/docs/Content/Overview/biometric-assurance.htm ("Liveness Assurance is a patented 3D passive face biometric verification technology that combines camera imagery and contextual data from the authentication process. Powerful deep learning AI methods assure accurate face matching and determine liveness."); **Liveness Assurance** Liveness Assurance is a patented 3D passive face biometric verification technology that combines camera imagery and contextual data from the authentication process. Powerful deep learning AI methods assure accurate face matching and determine liveness. LA has these benefits: • Delivers a simple, passive, and low ceremony user experience. • Provides assurance it's a **real** person and the **right** person. • Defends against known digital or physical presentation attacks and camera bypass digital attacks.

’606 Patent Claim Language	Accused Instrumentality
	The iProov Neural Network necessarily analyzes all data provided to it to verify to a high level of confidence that the user is three-dimensional. www.iproov.com/videos/liveness-assurance (the Accused Instrumentality confirms that a user is “a real person … [and] not a photograph.”). The iProov Neural Network verifies this based at least in part on analyzing the first data and the second data. The iProov Neural Network internally compares the first data and the second data to identify similarities and differences therebetween. This comparison includes (1) whether the first biometric data has differences from the second biometric data, and (2) whether the differences between the first biometric data and the second biometric data match expected differences between an image of a three-dimensional user’s face taken at the first distance and an image of a user’s three-dimensional face taken at the second distance. *See, e.g.*, IP-00003260; *see also* IP-00003256-61. The Accused Instrumentality requires no change (facial or otherwise) other than a change in distance (and potentially a realignment within the oval) between the user and the device.

determining that the user's face is three-dimensional when: the first biometric data is not identical to the second biometric data; and the second biometric data has expected differences as compared to the first biometric data, the expected differences resulting from the change in distance between the user and the camera when the at least one first image was captured at the first distance and the at least one second image was captured at the second distance.	As shown in the images reproduced above, the Accused Instrumentality necessarily requires that the first biometric data is not identical to the second biometric data. For example, the images below each necessarily have different biometric data:  In addition, unless expected differences between the first biometric data and the second biometric data are observed by the iProov Neural Network, the Accused Instrumentality normally will not confirm that the user is physically present. For example, the Accused Instrumentality will normally not confirm the user is physically present when a two-dimensional photo is used in a "spoof" attempt. *See*, *e.g.*, www.iproov.com/videos/liveness-assurance (the Accused Instrumentality confirms that a user is "a real person … [and] not a photograph."); *see also* IP-00003256-61. Conversely, FaceTec has tested the Accused Instrumentality and confirmed that if expected distortion between the first data and the second data matches expected distortion between an image of a user's three-dimensional face taken at the first distance and an image of a user's three-dimensional face taken at the second distance, the Accused Instrumentality will normally confirm the user's face is three-dimensional and that the user is likely to be physically present. For example, FaceTec tested the Accused Instrumentality and confirmed that Accused Instrumentality will

’606 Patent Claim Language	Accused Instrumentality
	normally confirm the user is physically present when a three-dimensional user conducts the verification steps outlined above. As shown in the images reproduced above, FaceTec tested the Accused Instrumentality using both a three dimensional “doll” head as well as a two-dimensional photo that had been modified with both a shawl and a pair of eyeglasses, both of which the Accused Instrumentality successfully verified.
20. The method of claim 19, wherein the receiving of the first biometric data and the second biometric data occurs at a server and the first biometric data and the second biometric data are received over one or more of a LAN, WAN, or Internet type network.	As shown in iProov’s data flow chart below, the iProov server receives from the user’s device “biometric data,” which is comprised of or based on the user’s face images captured by the Accused Instrumentality using the device’s camera, including the at least one first image and at least one second image of the user. This server receives this information over a network, which is a LAN, WAN, or Internet type network. *See* www.iproov.com/blog/cloud-biometrics-vs-on-device-difference (“At iProov, we believe that cloud-based, or server-side, biometric authentication is the only option to securely authenticate users remotely. If you use iProov, you are buying a cloud-hosted solution. … The entire authentication process happens server-side, independently from the device.”)  **Fig. 2: The Data Controller is iProov’s Customer, iProov is the Data Processor**

PROOF OF SERVICE

STATE OF CALIFORNIA, COUNTY OF ORANGE

I am employed in the County of Orange, State of California. I am over the age of 18 and not a party to the within action; my business address is 23 Corporate Plaza, Suite 150-105, Newport Beach, CA 92660.

On July 26, 2023, I caused the document(s) listed below to be served to the address(es) and by the method of service described as follows:

PLAINTIFF FACETEC, INC.'S AMENDED DISCLOSURE OF ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS

David W Gutke
Jay Joseph Schuttert
EVANS FEARS & SCHUTTERT LLP
6720 Via Austi Parkway
Suite 300
Las Vegas, NV 89119
702-805-0290
Fax: 702-805-0291
Email: dgutke@efstriallaw.com
Email: jschuttert@efstriallaw.com

Counsel for Defendant and Counter-Claimant, iProov Ltd

Alan Sege
ALAN SEGE, ESQ. PC
13323 West Washington Blvd.
Suite 302
Los Angeles, CA 90066
310-957-3301
Email: alan@alansege.com

Ryan E Hatch
HATCH LAW PC
13323 Washington Blvd.
Suite 302
Los Angeles, CA 90066
310-279-5076
Email: ryan@hatchlaw.com

[X] (BY EMAIL)

I declare that I am employed in the office of a member of the bar of this court at whose direction the service was made.

Executed on July 26, 2023,

Nate Lichtenberger